Jürgen Sander
Jörn Steuding
Rasa Steuding *Editors*

From Arithmetic to Zeta-Functions

Number Theory in Memory of Wolfgang Schwarz

Springer

From Arithmetic to Zeta-Functions

Jürgen Sander • Jörn Steuding • Rasa Steuding
Editors

From Arithmetic to Zeta-Functions

Number Theory in Memory of Wolfgang Schwarz

Springer

Editors
Jürgen Sander
Institut für Mathematik und Angewandte Informatik
Universität Hildesheim
Hildesheim, Germany

Jörn Steuding
Institut für Mathematik
Universität Würzburg
Würzburg, Germany

Rasa Steuding
Institut für Mathematik
Universität Würzburg
Würzburg, Germany

ISBN 978-3-319-28202-2 ISBN 978-3-319-28203-9 (eBook)
DOI 10.1007/978-3-319-28203-9

Library of Congress Control Number: 2016947422

Mathematics Subject Classification (2010): 11Axx, 11Bxx, 11Dxx, 11Jxx, 11Kxx, 11Lxx, 11Mxx, 11Nxx, 11Pxx, 01Axx

© Springer International Publishing Switzerland 2016
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Cover image: Illustration is published with kind permission of © Nicola Oswald, 2015.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Published with kind permission of © Jürgen Wolfart, 2009

Das schönste Denkmal, das ein Mensch bekommen kann, steht in den Herzen seiner Mitmenschen.[1]

Albert Schweitzer

[1]The most beautiful memorial which can be erected for somebody is the imprint he leaves behind in the hearts of others.

Wenn er aber studiert, müssen ihm bedeutende ideale Ziele vorschweben

The headline above is a passage from a personal statement written by Wolfgang Schwarz shortly after finishing school, explaining his views and goals while looking forward to taking up studies at the University of Erlangen. Literally, it says that a student's motivation must be substantial and idealistic. At that time it was customary to write a proposal for enrollment at a German university.

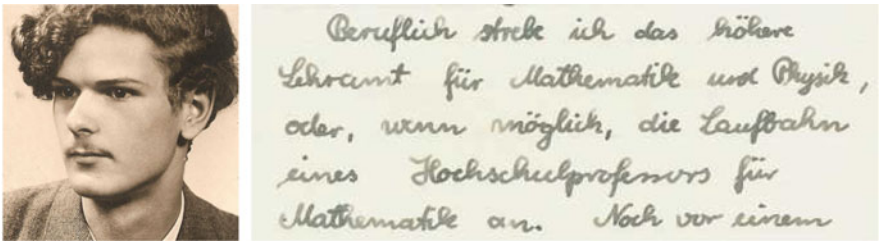

Beruflich strebe ich das höhere
Lehramt für Mathematik und Physik,
oder, wenn möglich, die Laufbahn
eines Hochschulprofessors für
Mathematik an. Noch vor einem

Fig. 1 *Left*: the 17-year-old Wolfgang Schwarz; *right*: excerpt from his essay. Published with kind permission of © Doris Schwarz, 2013

> As a profession I aim at the position of a high school teacher of mathematics and physics, or, if possible, the career of a university professor of mathematics.[2]

This is another quotation from Wolfgang Schwarz's essay showing a rather self-confident young man with ambitious goals. And indeed, this promising young man lived up to his own expectations and became an outstanding mathematician. His field of research was number theory with an emphasis on analysis. Yet, his interests were as widespread as his knowledge, ranging from elementary to algebraic aspects of number theory, and from analysis to algebra. This broad spectrum is well reflected

[2]This is our translation of the German original (see Fig. 1). Please note that the German *höheres Lehramt* stands for teaching pupils from grade 6 to 13 at a gymnasium, and *Hochschule* at that time was equivalent to university.

in the variety of research articles and surveys in this memorial volume, some of them enriched with personal reminiscences.

Wolfgang Schwarz was born on the 21st of April 1934 in Selb (not far from Hof in northern Bavaria), which is well known for its famous porcelain manufactories. His father was a teacher at a primary school and, although he died untimely in 1945 during World War II, he left a deep impression on young Wolfgang, which is best manifested in his early curiosity about mathematics and natural sciences. Their mother raised Wolfgang and his brother Werner and encouraged their musical talents. In 1951 Schwarz obtained his university entrance certificate, called *Reifezeugnis* in German. He enrolled at the Friedrich-Alexander-Universität Erlangen to study mathematics and physics; among his teachers were Otto Haupt, Georg Nöbeling, Wilhelm Specht, and, most importantly, the eminent Theodor Schneider, who is famous for his elegant solution of the seventh Hilbert problem on the transcendence of numbers of the form α^β, where α is algebraic and β irrational.[3] After passing the state examination for teachers in mathematics and physics in 1956 Wolfgang Schwarz continued his studies as an assistant of Schneider, first in Erlangen and later at the Albert-Ludwigs-Universität Freiburg (Fig. 2). His

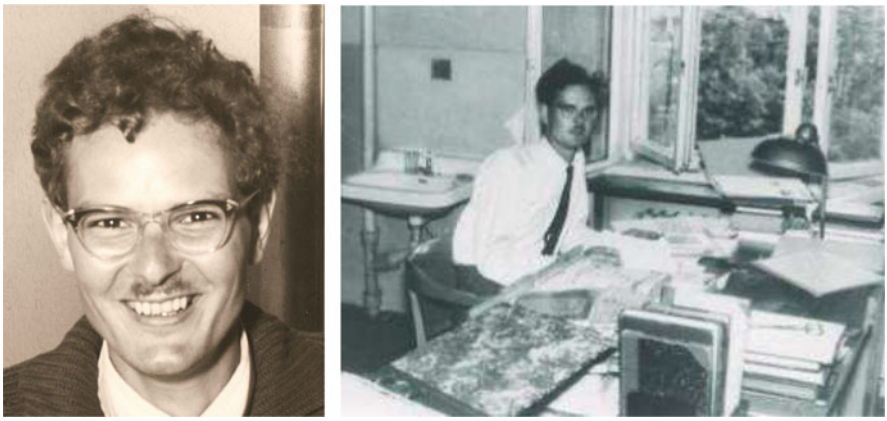


Fig. 2 Wolfgang Schwarz during his doctorate studies. Published with kind permission of © Doris Schwarz, 2013

doctorate thesis of 1959 dealt with questions about representations of integers as sums of powers of prime numbers. For his habilitation,[4] accomplished in 1964 also at Freiburg, he studied so-called Tauberian theorems with applications to partitions.

The topics and methods used in both of his theses form a central part of twentieth-century analytic number theory. In this memorial volume, honoring the life and work of Wolfgang

[3] Independently, Alexander Gelfond provided another solution about the same time.

[4] Habilitation is a degree following the doctorate, at that time necessary to obtain the permission for independent teaching (venia legendi) and for appointment as a professor.

Schwarz, the reader will find several contributions closely related to Schwarz's work, e.g. those by Jörg Brüdern, Rainer Dietmann & Christian Elsholtz, and Rebecca Ulrike Jakob, all relying on the circle method, as well as Aleksandar Ivić's article on Tauberian theorems. Some of these new results use or extend previous ones obtained by Schwarz. In the background of János Pintz's article on recent progress in the theory of prime number distribution are sieve methods, which is another direction of research where Schwarz made significant contributions and published monographs at an early age.

In the late 1960s Wolfgang Schwarz was appointed professor at the Albert-Ludwigs-Universität Freiburg, and in 1969 he became Ordinarius at the Johann-Wolfgang-Goethe-Universität Frankfurt. In 1974, he and his family settled in the village of Ruppertshain near Königstein in the lovely Taunus mountain range north of Frankfurt. The Schwarz family quickly became acquainted with its new surroundings and made many friends.

Wolfgang Schwarz's mathematical ideas and inventions were creative and innovative. His broad knowledge together with his mastery of advanced techniques was and still is very impressive. He always had a desire for simplicity and elegance. This is well reflected in his numerous (more than one hundred) research articles (see the complete list of his publications subsequent to this preface). A few of them deal with elementary, diophantine and transcendental questions.

The articles of Régis de la Bretèche & Gérard Tenenbaum, Štefan Porubský, Andrzej Schinzel, Jan-Christoph Schlage-Puchta, Tarlok Shorey & Rob Tijdeman, and Jürgen Spilker are elementary in nature and lie at the core of number theory. Diophantine aspects or transcendence topics are the major theme of the contributions by Ioulia Baoulina & Pieter Moree, Valentin Blomer, Yann Bugeaud, Peter Bundschuh & Keijo Väänänen, Carsten Elsner, Manfred Madritsch & Robert Tichy, and Jörn Steuding; some of them are directly related to results of Schwarz.

One of Wolfgang Schwarz's major research interests was the study of arithmetical functions. Together with his colleague and friend Jürgen Spilker from Freiburg, Schwarz published the standard reference in this field, continuing important works by Wintner, Delange, Wirsing, Elliott, and Halász. Methods of probabilistic and functional-analytic flavor form an essential part of Schwarz & Spilker's *Arithmetical Functions* and provide a rather new perspective on this classical topic. In particular, the concept of Ramanujan expansions, studies of so-called related functions, and Gelfand's theory of maximal ideal spaces make reading this book a great pleasure.

In this memorial volume several examples of recent and past work on arithmetical functions can be found in the articles of Peter Elliott, Karl-Heinz Indlekofer, Aleksandar Ivić, Lutz Lucht, Eugenijus Manstavičius, and Friedemann Tuttas, some of them directly related to Wolfgang Schwarz's work: the contribution by Aleksandar Ivić includes aspects of Schwarz's study of the value-distribution of certain arithmetical functions; the surveys of Lutz Lucht and Karl-Heinz Indlekofer discuss, among other topics, questions about inversion of multiplicative functions, resp. integration theory for arithmetical functions.

Wolfgang Schwarz has always been interested in establishing international contacts. He pursued this objective as one of the main organizers of the number theory meetings at Oberwolfach for two decades from 1974 until 1994 (together with

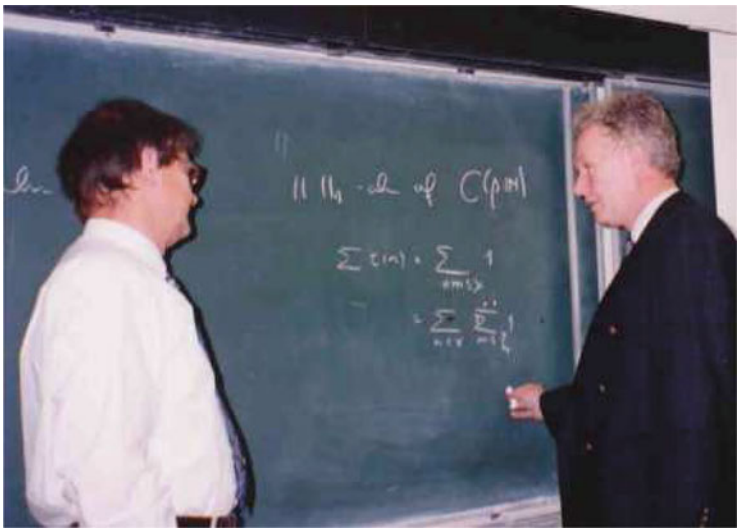


Fig. 3 Wolfgang Schwarz and his first doctoral student Karl-Heinz Indlekofer discussing the divisor function in 1993. Published with kind permission of © Karl-Heinz Indlekofer, 1993

Hans-Egon Richert and Eduard Wirsing). The success and worldwide reputation of these workshops in the Black Forest emphasize the mathematical significance of both Wolfgang Schwarz and the group of German number theorists at this time. Another notable activity of Schwarz was the exchange program with the group of probabilists and number theorists around Jonas Kubilius at Vilnius University (even before Lithuania's independence in 1990).

> In particular these Lithuanian contacts matched Schwarz's research interests on probabilistic number theory and applications to arithmetical functions, well reflected in the article by Eugenijus Manstavičius. However, questions around the Riemann zeta-function and its relatives should be mentioned here as well. To illustrate this line of research one may list the contributions of Ramūnas Garunkštis & Justas Kalpokas, and Antanas Laurinčikas. The article by Helmut Maier & Michael Rassias falls into this category, too. Another related paper by Nicola Oswald & Jörn Steuding traces this direction of investigation in the research area of the famous mathematician Adolf Hurwitz who was born in Hildesheim.[5] This article on the history of number theory reflects a further research interest of Wolfgang Schwarz.

After Wolfgang Schwarz's retirement in 2002, the history of mathematics and, in particular, the development of number theory, which he had always considered to play an important role in mathematical thinking and education, became the central topic of his mathematical activities. His extraordinary knowledge of mathematical and historical details often led to relevant and helpful remarks at conferences, more than once opening up a new point of view on a discussed unsolved problem or

[5]The town that hosted the 2014 $\mathcal{ELAZ}$ conference where the first steps for this memorial volume were initiated.

Fig. 4 Wolfgang Schwarz playing the piano. Published with kind permission of © Doris Schwarz, 2013

a presented result. Wolfgang Schwarz's other passion was classical music, which took an even larger role in his life as he was getting older. He played the piano to an almost professional level, and he composed his own pieces of music, which regularly have been performed by members of his family and also by students of the Hochschule für Musik und Darstellende Kunst Frankfurt (for example, to celebrate his 75th birthday).

Fig. 5 Eva Schwarz and Valentin Blomer playing one of Wolfgang Schwarz's pieces at the memorial colloquium during the 2014 $\mathcal{EIAZ}$ conference. Published with kind permission of © Isa Lange, 2014

On Friday, the 19th of July 2013, Wolfgang Schwarz passed away at the age of 79. During the biannual conference *Elementare und Analytische Zahlentheorie* ($\mathcal{ElAZ}$) hosted by the University of Hildesheim from July 26th to August 1st 2014, a special colloquium was held on Wednesday July 30th, dedicated to the memory of Wolfgang Schwarz. This was attended by his wife Doris and their daughter Eva, the conference delegates and several external guests. The idea to write a memorial volume to honor Schwarz's life and work was born at about the same time. The series of $\mathcal{ElAZ}$ conferences had been initiated by Lutz Lucht in 2000 in order to provide a regular platform for young German number theorists to present their research and to meet with experts. Since then these workshops have continued to grow into an international conference with eighty participants from all over the world, invited morning lectures and parallel sessions in the afternoons. The program of the Memorial Colloquium at the Hildesheim $\mathcal{ElAZ}$ together with a group photograph can be found on the final pages of this volume.

Besides Aleksandar Ivić's opening lecture as well as the Wednesday colloquium talks given by Lutz Lucht, Karl-Heinz Indlekofer, and Jörn Steuding honoring Schwarz's scientific work, this volume contains additional contributions presented at the $\mathcal{ElAZ}$ conference, some of them with personal reminiscences, for example, the one authored by Štefan Porubský.[6] The photograph on the previous page shows Valentin Blomer and Schwarz's daughter Eva playing one of Wolfgang Schwarz's own compositions during the memorial colloquium.

The third $\mathcal{ElAZ}$ conference held in Mainz in 2004 was organized by Wolfgang Schwarz and this is just one of the many examples showing his dedication to support young researchers. Another one is his longstanding commitment to the *Cusanuswerk* at the University of Frankfurt as a student mentor, a position he was committed to for more than 30 years. It is noteworthy that this Catholic institution is named after the fifteenth-century universal scientist and mathematician Nicholas of Cusa. Over the years Schwarz and his Cusanuswerk students met twice a year at his home for an evening of culture and good food prepared by Doris.

One of his students from the Cusanuswerk, Anne Henke, is now professor of mathematics and has contributed an article on her field of research, namely representation theory. This work as well as the articles by Samuel Patterson on variations of Gaussian sums, Jürgen Sander & Torsten Sander on the interaction between number theory and (algebraic) graph theory, Eduard Wirsing on a classical function-theoretical result of Hardy, and Jürgen Wolfart & Benjamin Mühlbauer on dessins d'enfants would most likely have met with Schwarz's enjoyment in the linkage of different mathematical views.

[6]The 'Obituary for Wolfgang Schwarz' by K.-H. Indlekofer, L.G. Lucht, and J. Steuding, published in *Jahresber. Dtsch. Math.-Ver.* **116**, No. 3, 153–169 (2014) provides further information.

Yet, Wolfgang Schwarz was not only a researcher and teacher of mathematics, he also was well aware of the importance of activities beyond the blackboard. He engaged in university administration and was a member of the presidium of the *Deutsche Mathematiker Vereinigung*[7] (DMV) for several years, being its president in 1986/1987. In 1992/1993 he was chairman of the *Konferenz der Mathematischen Fachbereiche*[8] (KMathF).

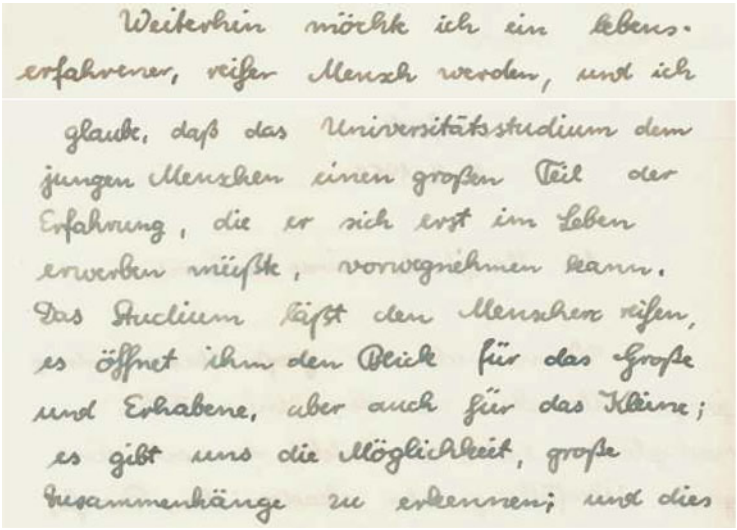

Weiterhin möchte ich ein lebens-
erfahrener, reifer Mensch werden, und ich
glaube, daß das Universitätsstudium dem
jungen Menschen einen großen Teil der
Erfahrung, die er sich erst im Leben
erwerben müßte, vorwegnehmen kann.
Das Studium läßt den Menschen reifen,
es öffnet ihm den Blick für das Große
und Erhabene, aber auch für das Kleine;
es gibt uns die Möglichkeit, große
Zusammenhänge zu erkennen; und dies

Fig. 6 Another quotation from Schwarz's essay of 1951. Published with kind permission of © Doris Schwarz, 2013

We conclude with a final quotation from Wolfgang Schwarz's essay for university entry:

> Furthermore I wish to become an experienced and mature man. I believe that by studying at a university, a young person is able to anticipate much of the experience he would otherwise have to accumulate later in life. By studying, humans gain maturity, it enables one to view the great and the sublime, but also the small; it provides us with the opportunity to see the big picture [...].

In our opinion, these words do not only show a young man's perspective towards his future life, but they also reflect the lifelong motto of a great character who had so much empathy and was so supportive of his colleagues and friends. The mathematical community has lost an excellent and renowned number theorist and

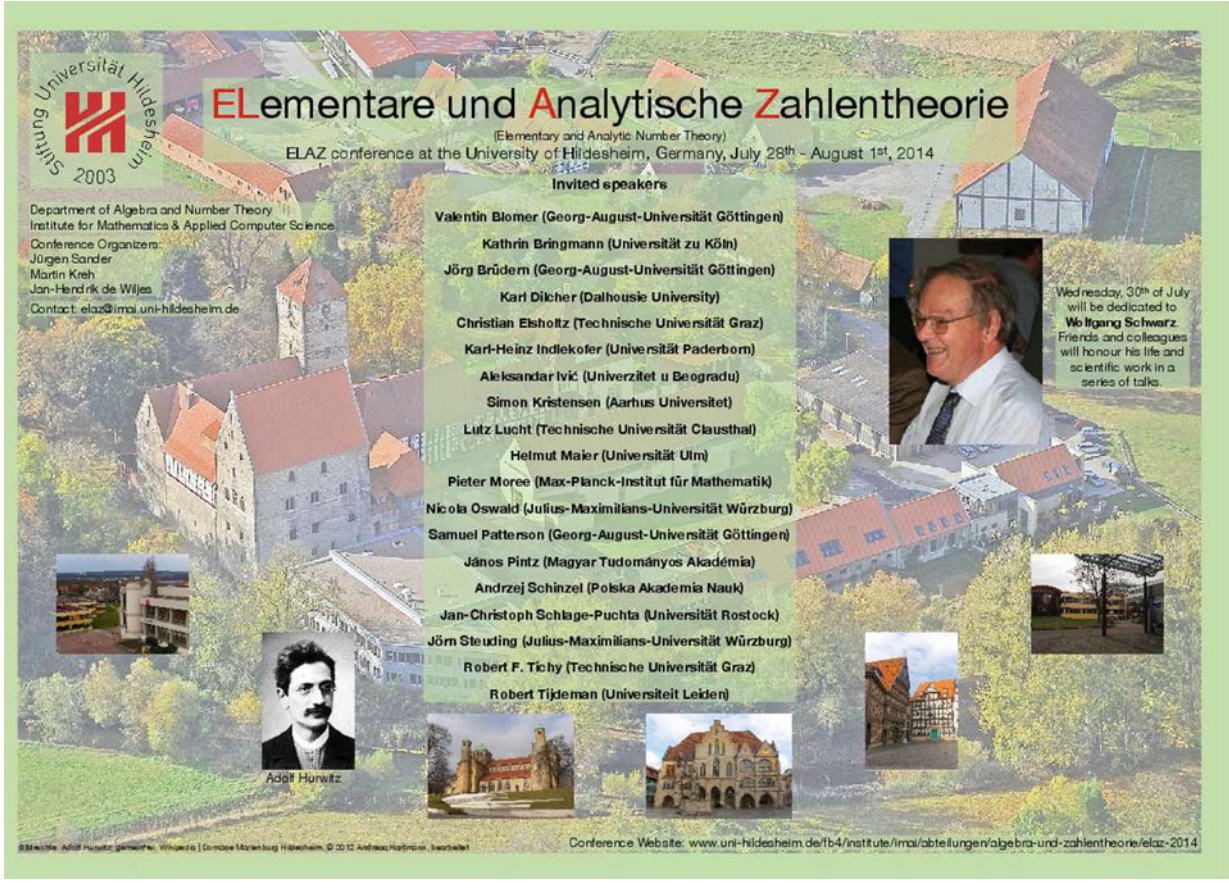
[7] Association of German Mathematicians.

[8] Literally the 'Conference of the mathematical faculties and departments' in Germany; there seems to be no English name.

a true friend. We will miss him while doing mathematics, making music, when playing chess or hiking, or simply in daily life.

Hildesheim — Jürgen Sander
Würzburg — Jörn and Rasa Steuding
November 2015

Post Scriptum: We are grateful to Doris Schwarz for providing us with biographical details, her husband's essay quoted above and several photographs, and to his daughter Karin Schwarz for proofreading. Further photographs in this volume have been contributed by friends and colleagues. We admire the artistic talent of Nicola Oswald, who created the watercoloured portrait of Wolfgang Schwarz on the front cover. Moreover, we thank Lutz Lucht for additional information as well as Karl Dilcher and Jan-Hendrik de Wiljes for technical support. Last but not least, we wish to express our gratitude to Mario Aigner, Sonja Gasser and the whole team at Springer Basel and Heidelberg for making our idea into a book.


Stiftung Universität Hildesheim 2003
ELementare und Analytische Zahlentheorie
(Elementary and Analytic Number Theory)
ELAZ conference at the University of Hildesheim, Germany, July 28th - August 1st, 2014
Invited speakers
Valentin Blomer (Georg-August-Universität Göttingen)
Kathrin Bringmann (Universität zu Köln)
Jörg Brüdern (Georg-August-Universität Göttingen)
Karl Dilcher (Dalhousie University)
Christian Elsholtz (Technische Universität Graz)
Karl-Heinz Indlekofer (Universität Paderborn)
Aleksandar Ivić (Univerzitet u Beogradu)
Simon Kristensen (Aarhus Universitet)
Lutz Lucht (Technische Universität Clausthal)
Helmut Maier (Universität Ulm)
Pieter Moree (Max-Planck-Institut für Mathematik)
Nicola Oswald (Julius-Maximilians-Universität Würzburg)
Samuel Patterson (Georg-August-Universität Göttingen)
János Pintz (Magyar Tudományos Akadémia)
Andrzej Schinzel (Polska Akademia Nauk)
Jan-Christoph Schlage-Puchta (Universität Rostock)
Jörn Steuding (Julius-Maximilians-Universität Würzburg)
Robert F. Tichy (Technische Universität Graz)
Robert Tijdeman (Universiteit Leiden)
Department of Algebra and Number Theory
Institute for Mathematics & Applied Computer Science
Conference Organizers:
Jürgen Sander
Martin Kreh
Jan-Hendrik de Wiljes
Contact: elaz@imai.uni-hildesheim.de
Wednesday, 30th of July will be dedicated to Wolfgang Schwarz. Friends and colleagues will honour his life and scientific work in a series of talks.
Adolf Hurwitz
Conference Website: www.uni-hildesheim.de/fb4/institute/imai/abteilungen/algebra-und-zahlentheorie/elaz-2014

The poster of the $\mathcal{ELAZ}$ conference in Hildesheim. Published with kind permission of © Jürgen Sander, 2014

Wolfgang Schwarz's Publications

1. Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. I. Darstellung hinreichend grosser Zahlen. *J. Reine Angew. Math.* **205** (1960/1961), 21–47.
2. Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. II. *J. Reine Angew. Math.* **206** (1961), 78–112.
3. Weitere, mit einer Methode von Erdös-Prachar erzielte Ergebnisse. *Math. Nachr.* **23** (1961), 327–348.
4. Über die Summe $\sum_{n\leq x} \varphi(f(n))$ und verwandte Probleme. *Monatsh. Math.* **66** (1962), 43–54.
5. Irrationale Potenzreihen. *Arch. Math.* **13** (1962), 228–240.
6. Zur Darstellung einer Zahl als Summe einer k-ten Potenz einer potenzfreien Zahl und einer g-ten potenzfreien Zahl. *Arch. Math.* **14** (1963), 105–115.
7. Eine Bemerkung über fast-ganzwertige Funktionen. *Monatsh. Math.* **67** (1963), 129–136.
8. Über die Lösbarkeit gewisser Ungleichungen durch Primzahlen. *J. Reine Angew. Math.* **212** (1963), 150–157.
9. Weitere, mit einer Methode von Erdös-Prachar erzielte Ergebnisse. II. *Monatsh. Math.* **68** (1964), 75–80.
10. *Einige Anwendungen Tauberscher Sätze in der Zahlentheorie*. Habilitationsschrift, Universität zu Freiburg i. Br., 1964.
11. Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. A. *J. Reine Angew. Math.* **219** (1965), 67–96.
12. Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. B. *J. Reine Angew. Math.* **219** (1965), 157–179.
13. Über die Anzahl Abelscher Gruppen gegebener Ordnung. I. *Math. Z.* **92** (1966), 314–320.
14. Einige Bemerkungen über periodische zahlentheoretische Funktionen. *Math. Nachr.* **31** (1966), 125–136.
15. Irrationale Potenzreihen. II. *Arch. Math.* **17** (1966), 435–437.
16. Über die Anzahl Abelscher Gruppen gegebener Ordnung. II. *J. Reine Angew. Math.* **228** (1967), 133–138.

17. Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. C. Mahler's Partitionsproblem. *J. Reine Angew. Math.* **228** (1967), 182–188.
18. Remarks on the irrationality and transcendence of certain series. *Math. Scand.* **20** (1967), 269–274.
19. Eine Bemerkung über die Anzahl der Zahlen pr^2 unterhalb x. *Colloq. Math.* **19** (1968), 117–120.
20. Schwache asymptotische Eigenschaften schnell wachsender multiplikativer zahlentheoretischer Funktionen. *Monatsh. Math.* **72** (1968), 355–367.
21. Schwache asymptotische Eigenschaften von Partitionen. *J. Reine Angew. Math.* **232** (1968), 1–16.
22. Der Primzahlsatz. *Überblicke Math.* **1** (1968), 35–61.
23. Asymptotische Formeln für Partitionen. *J. Reine Angew. Math.* **234** (1969), 174–178.
24. *Einführung in Ergebnisse und Methoden der Primzahltheorie*. BI Hochschultaschenbuch, Mannheim 1969.
25. Bemerkungen zu einem Satz der Herren Turán und Clunie über das Verhalten von Potenzreihen auf dem Rande des Konvergenzkreises. *Publ. Math. Debrecen* **16** (1969), 67–73.
26. Eine Bemerkung zu einer asymptotischen Formel von Herrn Rényi. *Arch. Math.* **21** (1970), 157–166.
27. Schwache asymptotische Eigenschaften von Partitionen. In: *Number Theory* (Colloq., János Bolyai Math. Soc., Debrecen, 1968) North-Holland, Amsterdam 1970, 191–196.
28. Über Teiler von n der Gestalt $p - 1$. In: *Zahlentheorie* (Tagung, Math. Forschungsinst., Oberwolfach, 1970), *Ber. Math. Forschungsinst.*, Oberwolfach **5**, Bibliographisches Inst., Mannheim, 1971, 147–158.
29. with Spilker, J.: Eine Anwendung des Approximationssatzes von Weierstrass-Stone auf Ramanujan-Summen. *Nieuw Arch. Wisk.* **19** (1971), 198–209.
30. Bemerkungen zu einem Satz der Herren Turán und Clunie über das Verhalten von Potenzreihen auf dem Rande des Konvergenzkreises. II. *Publ. Math. Debrecen* **18** (1971), 129–137.
31. Berichtigung zu der Arbeit "Weitere, mit einer Methode von Erdös-Prachar erzielte Ergebnisse". *Math. Nachr.* **52** (1972), 385.
32. A remark on multiplicative functions. *Bull. London Math. Soc.* **4** (1972), 136–140.
33. with Indlekofer, K.-H.: Über B-Zwillinge. *Arch. Math.* **23** (1972), 251–256.
34. Über B-Zwillinge. II. *Arch. Math.* **23** (1972), 408–409.
35. Ramanujan-Entwicklungen stark multiplikativer zahlentheoretischer Funktionen. *Acta Arith.* **22** (1973), 329–338.
36. with Wirsing, E.: The maximal number of non-isomorphic abelian groups of order n. *Arch. Math.* **24** (1973), 59–62.
37. Ramanujan-Entwicklungen stark multiplikativer Funktionen. *J. Reine Angew. Math.* **262/263** (1973), 66–73.
38. Eine weitere Bemerkung über multiplikative Funktionen. *Colloq. Math.* **28** (1973), 81–89.

39. with Wallisser, R.: Über gewisse nichtfortsetzbare Potenzreihen. *Monatsh. Math.* **77** (1973), 63–66
40. with Wallisser, R.: Über gewisse nichtfortsetzbare Potenzreihen. II. *Monatsh. Math.* **77** (1973), 251–266.
41. Über Potenzreihen, die irrationale Funktionen darstellen. I. *Überblicke Mathematik* **6** (1973), 179–196.
42. Die Ramanujan-Entwicklung reellwertiger multiplikativer Funktionen vom Betrage kleiner oder gleich Eins. *J. Reine Angew. Math.* **271** (1974), 171–176.
43. with Spilker, J.: Über zahlentheoretische Funktionen, die $f(x+y) = f(f(x) + f(y))$ erfüllen. *Mitt. Math. Sem. Giessen* **111** (1974), 80–86.
44. Über Potenzreihen, die irrationale Funktionen darstellen. II. *Überblicke Mathematik* **7** (1974), 7–32.
45. *Einführung in Siebmethoden der analytischen Zahlentheorie*. Bibliographisches Institut, Mannheim-Vienna-Zürich, 1974.
46. Über die Ramanujan-Entwicklung multiplikativer Funktionen. *Acta Arith.* **27** (1975), 269–279.
47. Eine Bemerkung über Restklassencharaktere. *Math.-Phys. Semesterber.* **22** (1975), 185–192.
48. Zum zahlentheoretischen Werk von Enrico Bombieri. *Überblicke Mathematik* **8** (1975), 150–151.
49. *Einführung in die Zahlentheorie*. Wissenschaftliche Buchgesellschaft, Darmstadt, 1975.
50. with Lucht, L.G.: Über die Lösungsanzahl der Gleichung $f(n) = \kappa \cdot n$ für gewisse Klassen multiplikativer Funktionen. *Monatsh. Math.* **81** (1976), 213–216.
51. Aus der Theorie der zahlentheoretischen Funktionen. *Jber. Deutsch. Math.-Verein.* **78** (1976/77), 147–167.
52. with Spilker, J.: Mean values and Ramanujan expansions of almost even arithmetical functions. In: *Topics in Number Theory* (Proc. Colloq., Debrecen, 1974), Colloq. Math. Soc. Janos Bolyai, Vol. 13, North-Holland, Amsterdam, 1976, 315–357.
53. Liouville-Zahlen und der Satz von Baire. *Math.-Phys. Semesterber.* **24** (1977), 84–87.
54. with Zassenhaus, H.: In Memoriam Bohuslav Diviš. *J. Number Theory* **9** (1977), v–vii.
55. Vanishing sums of roots of unity. *Elem. Math.* **33** (1978), 141–143.
56. Survey on analogues of the Waring problem: Diophantine inequalities. In: *Conference on Additive Number Theory* (Bordeaux, 1977), Univ. Bordeaux I, Talence, 1978, 121–147.
57. Periodic, multiplicative number-theoretical functions. *Monatsh. Math.* **87** (1979), 65–67.
58. with Kopetzky, H.G.: Two conjectures of B. R. Santos concerning totitives. *Math. Comp.* **33** (1979), 841–844.

59. Some applications of Elliott's mean-value theorem. *J. Reine Angew. Math.* **307/308** (1979), 418–423.
60. with Spilker, J.: Wiener-Lévy-Sätze für absolut konvergente Reihen. *Arch. Math.* **32** (1979), 267–275.
61. with Ivić, A.: Remarks on some number-theoretical functional equations. *Aequationes Math.* **20** (1980), 80–89.
62. with Duttlinger, J.: Über die Verteilung der pythagoräischen Dreiecke. *Colloq. Math.* **43** (1980), 365–372.
63. with Kopetzky, H.G., Wirsing, E.: Nonnegative sums of roots of unity. *Arch. Math.* **34** (1980), 114–121.
64. Fourier-Ramanujan-Entwicklungen zahlen-theoretischer Funktionen und Anwendungen. In: *Festschrift of the 75th Jubilee of the Scientific Society at the Johann Wolfgang Goethe-Universität*, Frankfurt/Main, Steiner, Wiesbaden 1981, 399–415.
65. with Knopfmacher, J.: Binomial expected values of arithmetical functions. *J. Reine Angew. Math.* **328** (1981), 84–98.
66. with Spilker, J.: Remarks on Elliott's theorem on mean-values of multiplicative functions. In: *Recent Progress in Analytic Number Theory*, Durham 1979, 1981, 325–339.
67. with Spilker, J.: Eine Bemerkung zur Charakterisierung der fast-periodischen multiplikativen zahlentheoretischen Funktionen mit von Null verschiedenem Mittelwert. *Analysis* **3** (1983), 205–216.
68. with Heppner, E.: Benachbarte multiplikative Funktionen. *Studies in Pure Mathematics*, 323–336, Birkhäuser, Basel, 1983.
69. with Waterhouse, W.C.: The asymptotic density of supersingular Fermat varieties. *Arch. Math.* **43** (1984), 142–144.
70. with Knopfmacher, J.: Binomial expected values of arithmetical functions. II. In: *Topics in Classical Number Theory*, Vol. I, II (Budapest, 1981), 863–905, Colloq. Math. Soc. János Bolyai, 34, North-Holland, Amsterdam, 1984.
71. with Herzog, J.: Über eine spezielle Partitionenfunktion, die mit der Anzahl der abelschen Gruppen der Ordnung n zusammenhängt. *Analysis* **5** (1985), 153–161.
72. Über einige Probleme aus der Theorie der Primzahlen. *Sitzungsber. Wiss. Ges. Johann Wolfgang Goethe-Univ. Frankfurt am Main* **21** (1985), 61–118.
73. Another evaluation of an Erdös-Turán constant. *Analysis* **5** (1985), 343–345.
74. Remarks on the theorem of Elliott and Daboussi, and applications. In: *Elementary and Analytic Theory of Numbers* (Warsaw, 1982), 463–498, Banach Center Publ., **17**, PWN, Warsaw, 1985.
75. *Beispiele und BASIC-Programme zum Mathematikunterricht*. Bibl. Inst. Mannheim 1985.
76. with Spilker, J.: A variant of proof of Daboussi's theorem on the characterization of multiplicative functions with nonvoid Fourier-Bohr-spectrum. *Analysis* **6** (1986), 237–249.
77. A correction to: "Remarks on Elliott's theorem on mean-values of multiplicative functions" (Durham, 1979) and Some remarks on almost-even

number-theoretical functions. In: *Analytic and Elementary Number Theory* (Marseille, 1983), 139–158, Publ. Math. Orsay, 86-1, Univ. Paris XI, Orsay, 1986.
78. with Porubský, Š.: Sums of additive functions on arithmetical semigroups. *Colloq. Math.* **53** (1987), 137–146.
79. Almost-even number-theoretical functions. In: *Probability Theory and Mathematical Statistics*, Vol. II (Vilnius, 1985), 581–587, VNU Sci. Press, Utrecht, 1987.
80. Bildungsinhalte des Mathematik-Studiums. In: Die Bildungswerte des Studiums Mathematisch-Naturwissenschaftlicher Fächer, WRK, *Dokumente z. Hochschulreform* 64/1988, 1987, 37–67.
81. Ramanujan expansions of arithmetical functions. In: *Ramanujan Revisited* (Urbana-Champaign, Ill., 1987), 187–214, Academic Press, Boston, MA, 1988.
82. with Hildebrand, A., Spilker, J.: Still another proof of Parseval's equation for almost-even arithmetical functions. *Aequationes Math.* **35** (1988), 132–139.
83. with Kappe, L.-Ch., Schlickewei, H.P.: Theodor Schneider zum Gedächtnis. *Jahresber. Deutsch. Math.-Verein.* **92** (1990), 111–129.
84. Geschichte der analytischen Zahlentheorie seit 1890. In: *Ein Jahrhundert Mathematik 1890–1990*, 741–780, Dokumente Gesch. Math., 6, Vieweg, Braunschweig, 1990.
85. with Maxsein, T., Smith, P.: An example for Gelfand's theory of commutative Banach algebras. *Math. Slovaca* **41** (1991), 299–310.
86. with Maxsein, T.: A new proof of a theorem concerning functions in different spaces of almost-periodic arithmetical functions. *Proceedings of the Amalfi Conference on Analytic Number Theory* (Maiori, 1989), 315–323, Univ. Salerno, Salerno, 1992.
87. Emeritierung von Friedrich Hirzebruch. *Mitt. Dt. Math. Ver.* 1993-2, 32–33.
88. with Spilker, J.: *Arithmetical Functions: An Introduction to Elementary and Analytic Properties of Arithmetic Functions and to Some of their Almost-Periodic Properties.* Cambridge University Press, 1994.
89. Some remarks on the history of the prime number theorem from 1896 to 1960. In: *Development of Mathematics 1900–1950*, ed. J.-P. Pier, Birkhäuser 1994 (Symposium Luxembourg 1992), 565–615.
90. Some aspects of the development of probabilistic number theory. In: *Probability Theory and Mathematical Statistics* (Vilnius, 1993), 661–701, TEV, Vilnius, 1994.
91. with Tschiersch, R.: *Studienführer Mathematik*. Karl Bock Verlag, Bad Honnef, 1994.
92. Die Mathematik gleicht einem Baum. *Forschung & Lehre* 10/1994, 434–437, Bonn.
93. Evaluation of mean-values of products of shifted arithmetical functions. *Note Mat.* **15** (1995), 235–250 (1997).

94. with Spilker, J.: A remark on some special arithmetical functions. In: *New Trends in Probability and Statistics* **4** (Palanga, 1996), 221–245, VSP, Utrecht, 1997.
95. On the number-theoretical work of Edmund Hlawka. In: *Proc. Conf. Analytic and Elementary Number Theory*, Vienna, July 18–20, 1996, 1–30, Universität Wien and Universität für Bodenkultur, Wien, 1997.
96. Wirsing's theorems; Delange's theorem; Elliott-Daboussi theorem; Halász' mean value theorem. Contributions to *Encyclopaedia of Mathematics*, Supplement I, Kluwer Academic Publishers, 1997.
97. with Burde, G.: Wolfgang Franz zum Gedächtnis. *Jahresber. Deutsch. Math.-Verein.* **100** (1998), 284–292.
98. Evaluation of mean-values of products of shifted arithmetical functions. II. In: *Number theory in progress*, Vol. 2 (Zakopane-Kościelisko, 1997), 1081–1098, de Gruyter, Berlin, 1999.
99. Nachruf auf Wolfgang Franz. *Sitzungsber. Wiss. Gesellschaft Frankfurt* XXXVI (1999), 379–383.
100. Some Results on Arithmetical Functions. In: *Prob. Theory and Math. Stat.*, Proc. 7th Internat. Vilnius Conference, August 12–18, 1998, Utrecht 1999, 653–664.
101. Almost-even functions as solutions of a linear functional equation. *Math. Slovaca* **50** (2000), 525–529.
102. Uniform-fast-gerade Funktionen mit vorgegebenen Werten. *Arch. Math.* **77** (2001), 1–4.
103. John Knopfmacher, analytic number theory, and the theory of arithmetical functions. *Quaest. Math.* **24** (2001), 273–290.
104. Zur Entwicklung einiger Gebiete der Zahlentheorie, insbesondere im 19. Jahrhundert. *Sitzungsber. Wiss. Ges. Univ. Frankfurt* XXXIX (2001), 75–123.
105. with Choi, E.-H.: Mean-values of products of shifted arithmetical functions. In: *Analytic and Probabilistic Methods in Number Theory* (Palanga, 2001), 32–41, TEV, Vilnius, 2002.
106. with Laurinčikas, A., Steuding, J.: Value distribution of general Dirichlet series. III. In: *Analytic and Probabilistic Methods in Number Theory* (Palanga, 2001), 137–156, TEV, Vilnius, 2002.
107. with Burde, G., Wolfart, J.: Ein Mathematiker mit universalem Anspruch. Über Max Dehn und sein Wirken am Mathematischen Seminar. *Forschung Frankfurt* 4/2002, 85–89.
108. with Laurinčikas, A., Steuding, J.: The universality of general Dirichlet series. *Analysis* **23** (2003), 13–26.
109. with Volkmann, B.: Hans Rohrbach zum Gedächtnis 27.2.1903–19.12.1993. *Jahresber. Deutsch. Math.-Verein.* **105** (2003), 89–99.
110. with Spilker, J.: Uniform-fast-gerade Funktionen mit vorgegebenen Werten. II. *Arch. Math.* **81** (2003), 534–537.

111. with Schlage-Puchta, J.-C., Spilker, J.: Uniformly-almost-even functions with prescribed values. III. *Ann. Univ. Sci. Budapest. Sect. Comput.* **22** (2003), 317–330.
112. with Schlage-Puchta, J.-C., Spilker, J.: Uniformly-almost-even functions with prescribed values. IV. Application of Gelfand theory. *Analysis* **24** (2004), 63–70.
113. with G. Burde, G., Wolfart, J.: Max Dehn und das Mathematische Seminar der Universität Frankfurt. Mathematik im Fluss der Zeit. *Algorismus* 44 (2004), 462–483.
114. *Aus der Geschichte der Frankfurter Mathematik. Festschrift zu den 100. Geburtstagen von Ruth Moufang, Gottfried Köthe, Wolfgang Franz*. Edited by Wolfgang Schwarz. *Schriften des Universitätsarchivs Frankfurt am Main*, 1, 2005.
115. with Wolfart, J.: Drei Säulen des Frankfurter Mathematischen Seminars. *Forschung Frankfurt* 2/2005, 55–59.
116. *Elementare und Analytische Zahlentheorie*. Proceedings of the 3rd Conference (ELAZ) held in Mainz, May 24–28, 2004. Edited by Wolfgang Schwarz and Jörn Steuding. Schriften Wiss. Ges. Johann Wolfgang Goethe-Universität Frankfurt am Main, Franz Steiner Verlag Stuttgart, Stuttgart, 2006.
117. with Lucht, L.G.: Zum Gedenken an Thomas Maxsein. In: *Elementare und Analytische Zahlentheorie*, 346–348, Schriften Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, Franz Steiner Verlag Stuttgart, Stuttgart, 2006.
118. with Steuding, R., Steuding, J.: Universality for Euler products, and related arithmetical functions. In: *Analytic and Probabilistic Methods in Number Theory* (Palanga 2006), 163–189, TEV, Vilnius, 2007.
119. Some highlights from the history of probabilistic number theory. In: *Probability and Number Theory*, Kanazawa 2005, 367–419, *Adv. Stud. Pure Math.* **49**, Math. Soc. Japan, Tokyo, 2007.

Impressions

Mathematicians in general are sociable people. They meet at conferences and discuss their latest results and much more at conference dinners.

Published with kind permission of © Stefan Porubsky, 2004

The picture above shows Wolfgang Schwarz hosting a number theoretical meeting in Frankfurt in summer 2004, surrounded by (from left to right) Aleksandar Ivić, Antanas Laurinčikas, Jörn Steuding, Štefan Porubský, and Jürgen Wolfart.

Below a scene from a private round at Schwarz's home in the Taunus village Ruppertshain with guests. From left to right: Aleksandar Ivić, Andrzej Schinzel, Štefan Porubský, János Pintz, Wolfgang Schwarz, and Antanas Laurinčikas.

Published with kind permission of © Stefan Porubsky, 2004

Published with kind permission of © Stefan Porubsky, 1989

The photograph above shows Wolfgang Schwarz discussing mathematics with Karl Dilcher. In the next one, Rasa Steuding, Karl-Heinz Indlekofer, Kohji Matsumoto,

Wolfgang Schwarz, and Eugenijus Manstavicius (from left to right) having dinner in a Japanese restaurant.

Published with kind permission of © Jörn Steuding, 2005

The following photograph shows Wolfgang Schwarz during the 2012 $\mathcal{ELAZ}$ Conference at Schloß Schney talking with Lutz Lucht and his wife.

Published with kind permission of © Stefan Porubsky, 2012

Professer Schwarz discussing mathematics with his colleagues Profs. Albrecht Pfister (left) and Jürgen Spilker (right).

Published with kind permission of © Jürgen Wolfart, 2009

Below another example, Wolfgang Schwarz in discussion with Eugenijus Manstavicius; in the background Jürgen Sander (on the left) and Eduard Wirsing (in the middle).

Published with kind permission of © Stefan Porubsky, 2012

But sometimes mathematicians are silently watching someone else's talk. The next photograph shows Günter Pickert, Eduard Wirsing, Wolfgang Schwarz, and

Karl-Heinz Indlekofer (from left to right).

Published with kind permission of © Jürgen Wolfart, 2009

Some mathematicians are genuine globetrotters. Wolfgang Schwarz was one of those, and he was a passionate alpinist and mountaineer (see the photographs in Lutz Lucht's contribution).

Published with kind permission of © Peter Elliott, 1975

The last - rather romantic - photograph shows him at the Glaswaldsee in the Black Forest, while the photograph below, showing Wolfgang and Doris Schwarz, was taken during a rainy day at the Curonian Spit in Lithuania.

Published with kind permission of © Jörn Steuding, 2011

The Schwarz family has always been very hospitable. Below a photo showing the beginning of an excursion of a larger group of tourists in the Taunus range 2004.

From left to right: Wolfgang Schwarz, Jörn Steuding, Andrzej Schinzel, Doris Schwarz, János Pintz, Aleksandar Ivić, and Antanas Laurinčikas. Published with kind permission of © Stefan Porubsky, 2004

At conferences mathematicians give and listen to talks.

Published with kind permission of © Jürgen Wolfart, 2009

Eduard Wirsing (on the left) and Wolfgang Schwarz enjoying a humoristic moment at the $\mathcal{ELAZ}$ Conference 2012 in Schloß Schney.

Sometimes there are moments for celebration. At the $\mathcal{ELAZ}$ Conference 2004

Published with kind permission of © Stefan Porubsky, 2004

in Mainz Wolfgang Schwarz was celebrating his 70th birthday. As a representative of the Lithuanian delegation Eugenijus Manstavicius is handing over a hand-made Lithuanian sash.

Group photographs are another favourite amusement of mathematicians during their meetings.

Published with kind permission of © Peter Elliott, 1984

These pictures show Wolfgang Schwarz, Peter Elliott, Dieter Wolke, Ernst Heppner, Karl-Heinz Indlekofer, and Imre Katai (above from left to right) as well as Gérald Tenenbaum, once again Schwarz, Richard Warlimont, and Lutz Lucht (below from left to right) at a number theory conference at the Mathematisches Forschungsinstitut Oberwolfach in 1984.

Published with kind permission of © Peter Elliott, 1984

Published with kind permission of © Stefan Porubsky, 2012

Wolfgang Schwarz answering questions after his talk at the $\mathcal{EL}\mathcal{AZ}$ Conference 2012 in Schloß Schney. In the background chairman Jürgen Sander.

At such occasions one can sometimes meet other mathematician's families. Wolfgang Schwarz and part of the Porubský family having coffee and ice cream.

Published with kind permission of © Stefan Porubsky, 1991

Contents

Wenn er aber studiert, müssen ihm bedeutende ideale Ziele vorschweben vii

Wolfgang Schwarz's Publications xvii

Impressions xxv

Forbidden Integer Ratios of Consecutive Power Sums 1
Ioulia N. Baoulina and Pieter Moree

A Note on the Negative Pell Equation 31
Valentin Blomer

Localisation Conditionnelle de Diviseurs 41
Régis de la Bretèche and Gérald Tenenbaum

A Ternary Problem in Additive Prime Number Theory 57
Jörg Brüdern

An Improvement of Liouville's Inequality 83
Yann Bugeaud

Guided by Schwarz' Functions: A Walk Through the Garden of Mahler's Transcendence Method 91
Peter Bundschuh and Keijo Väänänen

Sums of Two Squares and a Power 103
Rainer Dietmann and Christian Elsholtz

Multiplicative Functions and the Sign of Maass Form Fourier Coefficients 109
Peter D.T.A. Elliott

On Error Sum Functions for Approximations with Arithmetic Conditions 121
Carsten Elsner

Sum of the Lerch Zeta-Function over Nontrivial Zeros of the Dirichlet *L*-Function 141
Ramūnas Garunkštis and Justas Kalpokas

Schur–Weyl Dualities Old and New 155
Anne Henke

Arithmetic Functions: A Pivotal Topic in the Scientific Work of Wolfgang Schwarz 179
Karl-Heinz Indlekofer

On Some Selected Works of Wolfgang Schwarz 201
Aleksandar Ivić

Sums of Two Squares of Sums of Two Squares 217
Rebecca Ulrike Jakob

The Joint Discrete Universality of Periodic Zeta-Functions 231
Antanas Laurinčikas

Remembering Wolfgang Schwarz, His Life and Work 247
Lutz G. Lucht

Dynamical Systems and Uniform Distribution of Sequences 263
Manfred G. Madritsch and Robert F. Tichy

Asymptotics and Equidistribution of Cotangent Sums Associated with the Estermann and Riemann Zeta Functions 277
Helmut Maier and Michael Th. Rassias

A Turán-Kubilius Inequality on Mappings of a Finite Set 295
Eugenijus Manstavičius

Aspects of Zeta-Function Theory in the Mathematical Works of Adolf Hurwitz 309
Nicola Oswald and Jörn Steuding

Selberg Sums: A New Perspective 353
Samuel J. Patterson

Polignac Numbers, Conjectures of Erdős on Gaps Between Primes, Arithmetic Progressions in Primes, and the Bounded Gap Conjecture 367
János Pintz

Idempotents and Congruence $ax \equiv b \pmod{n}$ 385
Štefan Porubský

Recent Developments on the Edge Between Number Theory and Graph Theory 405
Jürgen Sander and Torsten Sander

The Leading Coefficients of Stern Polynomials 427
Andrzej Schinzel

The Non-existence of Universal Carmichael Numbers 435
Jan-Christoph Schlage-Puchta

Arithmetic Properties of Blocks of Consecutive Integers 455
Tarlok N. Shorey and Rob Tijdeman

The GCD of the Shifted Fibonacci Sequence 473
Jürgen Spilker

On Liouville Numbers: Yet Another Application of Functional Analysis to Number Theory 485
Jörn Steuding

Natural Boundaries of Power Series with Multiplicative Coefficients in Algebraic Number Fields 509
Friedemann Tuttas

A Minimal Proof of a Result of Hardy 523
Eduard Wirsing

Regular Dessins with Abelian Automorphism Groups 527
Jürgen Wolfart and Benjamin Mühlbauer

Impressions from the $\mathcal{ELAZ}$ Conference 2014 in Hildesheim 535

Forbidden Integer Ratios of Consecutive Power Sums

Ioulia N. Baoulina and Pieter Moree

To the memory of Prof. Wolfgang Schwarz

Abstract Let $S_k(m) := 1^k + 2^k + \cdots + (m-1)^k$ denote a power sum. In 2011 Bernd Kellner formulated the conjecture that for $m \geq 4$ the ratio $S_k(m+1)/S_k(m)$ of two consecutive power sums is never an integer. We will develop some techniques that allow one to exclude many integers ρ as a ratio and combine them to exclude the integers $3 \leq \rho \leq 1501$ and, assuming a conjecture on irregular primes to be true, a set of density 1 of ratios ρ. To exclude a ratio ρ one has to show that the Erdős–Moser type equation $(\rho-1)S_k(m) = m^k$ has no non-trivial solutions.

Keywords Consecutive power sums • Erdős–Moser type equation

2010 Mathematics subject classification: Primary 11D61; Secondary 11A07

1 Introduction

Power sums have fascinated mathematicians for centuries. In this paper we consider some Diophantine equations involving power sums, of which the Erdős–Moser equation

$$1^k + 2^k + \cdots + (m-2)^k + (m-1)^k = m^k \tag{1.1}$$

I.N. Baoulina
Department of Mathematics, Moscow State Pedagogical University,
Krasnoprudnaya str. 14, Moscow 107140, Russia
e-mail: jbaulina@mail.ru

P. Moree (✉)
Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany
e-mail: moree@mpim-bonn.mpg.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_1

is typical and the most famous one. This equation has the obvious solution $(m, k) = (3, 1)$ and conjecturally no other solutions exist (this conjecture was formulated around 1950 by Paul Erdős in a letter to Leo Moser). Leo Moser [20], using only elementary number theory, established the following result.

Theorem 1.1 (Leo Moser [20]) *If (m, k) is a solution of (1.1) with $k \geq 2$, then $m > 10^{10^6}$.*

For the shortest proof of this result presently known, we refer to Moree [16].

Using very different techniques, namely continued fractions and a many decimal computation of $\log 2$, Gallot et al. [6] established the current world record:

Theorem 1.2 (Gallot et al. [6]) *If an integer pair (m, k) with $k \geq 2$ satisfies (1.1), then*

$$m > 2.7139 \cdot 10^{1\,667\,658\,416}.$$

The bound $m > 10^{10^{10}}$ seems feasible, but requires somewhat better computer resources than the authors of [6] had at their disposal.

Let $S_k(m) := \sum_{j=1}^{m-1} j^k$ be the sum of the first $m-1$ consecutive kth powers. In this notation we can rewrite (1.1) as

$$S_k(m) = m^k. \tag{1.2}$$

In the literature also the *generalized Erdős–Moser* conjecture is considered. The strongest result to date is due to the second author [17] who proved the following.

Theorem 1.3 *For a fixed positive integer a, the equation $S_k(m) = am^k$ has no integer solutions (m, k) with*

$$k \geq 2, \quad m < \max\left(10^{9\cdot 10^6}, a \cdot 10^{28}\right).$$

Interestingly, the method of Gallot et al. allows one only to deal with a specific value of a, for a general a only the elementary method of Moser is available.

Kellner [10] conjectured that if k and m are positive integers with $m \geq 3$, the ratio $S_k(m+1)/S_k(m)$ is an integer iff $(m, k) \in \{(3, 1), (3, 3)\}$. Noting that $S_k(m+1) = S_k(m) + m^k$, one observes that this conjecture is equivalent with the following one.

Conjecture 1.4 (Kellner–Erdős–Moser) *Let $m \geq 3$. We have*

$$aS_k(m) = m^k \tag{1.3}$$

iff $(a, m, k) \in \{(1, 3, 1), (3, 3, 3)\}$.

If this conjecture holds true, then obviously so does the Erdős–Moser conjecture. However, whereas the Erdős–Moser conjecture is open, we are able to establish the unsolvability of (1.3) for many integers a.

Theorem 1.5 *If a has a regular prime as divisor or $2 \le a \le 1500$, then the equation $aS_k(m) = m^k$ has no solution with $m \ge 4$.*

(We consider 2 to be a regular prime, see Sect. 2 for details.) The first restriction on a is not very difficult to prove, but powerful in its consequences. Assume that there exists a real number $\delta < 1$ such that the number of irregular primes $p \le x$ is bounded above by $\delta x/\log x$ as $x \to \infty$. It then follows (see Sect. 2) that, for a set of integers a of density 1, $aS_k(m) = m^k$ has no solution with $m \ge 4$. The first restriction implies that in order to exclude the a in the range $2 \le a \le 1500$, one has to exclude $a = 37^2$ and all irregular primes in this interval. These a can be dealt with using various technical and not very general necessary conditions for (1.3) to be solvable.

In case we are not able to exclude a square-free a, we are able to show that if (1.3) holds, then both k and m are large.

Theorem 1.6 *Suppose that $aS_k(m) = m^k$, $m \ge 4$ and a is square-free, then both k and m exceed $3.44 \cdot 10^{82}$.*

We would like to point out that for solutions with $m \equiv 1 \pmod 3$ or $m \equiv 1 \pmod{30}$ much larger lower bounds hold true (see Theorem 8.4).

For a fixed integer $a \ge 1$ it is not known whether there are finitely many solutions (m, k) of (1.3) or not. In this direction we can only contribute the following modest result.

Proposition 1.7 *Let (m_1, k_1) and (m_2, k_2) be different solutions of $aS_k(m) = m^k$. Then $m_1 \ne m_2$ and $k_1 \ne k_2$.*

A final approach for dealing with Eq. (1.3) is to try to prove that k is divisible by 120 say. Once established, there are many options on how to get an even bigger number to divide k. A cascade of ways how to proceed further arises and it seems very likely then that also in this case $a + 1$ cannot occur as a ratio. We demonstrate this cascade process in Sect. 7. Paul Tegelaar [24] jokingly called this 'the method of infinite ascent'.

After discussing some basic material on Bernoulli numbers and power sums in Sect. 2, we obtain a crucial result (Theorem 3.11) relating Bernoulli numbers and solutions of the Kellner–Erdős–Moser equation in Sect. 3. Integers a that are a product of irregular primes cannot be immediately excluded, and for these one can use *helpful pairs*, see Sect. 4. They allow one to rule out that $k \equiv c \pmod d$ for many even integers $c \ge 2$ and d. In Sect. 5 we demonstrate with both an easy and a difficult example how to exclude a given integer ratio ρ. Table 3 in Appendix illustrates in a compact way how to show that $3 \le \rho \le 1501$ are forbidden ratios. Some ratios are clearly much easier to exclude than others and this is discussed in Sect. 6. In Sect. 7 we discuss how to show that a given integer divides k. In Sect. 8 we reason in the way of Moser to derive lower bounds for k and m in case a is squarefree. In Sect. 9 proofs of the new results announced above are given. These are mainly based on work done in earlier sections. In the final section, Sect. 10, some further properties of potential solutions of the Kellner–Erdős–Moser equation

are derived. The proof that the integers $2 \leq a \leq 1500$ are forbidden makes use of Tables 2 and 3 in Appendix.

A survey of earlier work on Erdős–Moser type conjectures can be found in Moree [17], also see [3, Chap. 8], for an expository account of the work of Gallot et al. [6].

2 Preliminaries on Bernoulli Numbers and Power Sums

Lemma 2.1 (Carlitz–von Staudt) *Let k and m be positive integers, then*

$$S_k(m) = \sum_{j=1}^{m-1} j^k \equiv \begin{cases} 0 \pmod{\frac{m(m-1)}{2}} & \text{if } k \text{ is odd,} \\ -\sum_{p|m,(p-1)|k} \frac{m}{p} \pmod{m} & \text{otherwise.} \end{cases}$$

This result, with some small error (cf. Moree [14]), was published in 1961 by Carlitz. For an easy reproof of the above result, see Moree [16].

Recall that the *Bernoulli numbers* B_k are defined by the power series

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k t^k}{k!}.$$

They are rational numbers and can be written as $B_k = U_k/V_k$, with $V_k > 0$ and $\gcd(U_k, V_k) = 1$. One has $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$ and $B_{2j+1} = 0$ for $j \geq 1$.

In the next four lemmas, we record some well-known facts about the Bernoulli numbers (see [7, Chap. 15]).

Lemma 2.2 (von Staudt–Clausen) *If $k \geq 2$ is even, then $V_k = \prod_{(p-1)|k} p$.*

Lemma 2.3 (Kummer Congruence) *Let $k \geq 2$ be even and p be a prime with $(p-1) \nmid k$. If $k \equiv r \pmod{p-1}$, then $B_k/k \equiv B_r/r \pmod{p}$.*

Lemma 2.4 *For any integers $k \geq 1$ and $m \geq 2$,*

$$S_k(m) = \sum_{j=0}^{k} \binom{k}{j} B_{k-j} \frac{m^{j+1}}{j+1}.$$

Lemma 2.5 (Voronoi Congruence) *Let k and m be positive integers, where $m \geq 2$ and $k \geq 2$ is even, then $V_k S_k(m) \equiv U_k m \pmod{m^2}$.*

The following lemma gives a refinement of the Voronoi congruence (see [9, Proposition 8.5]).

Lemma 2.6 *Let k and m be positive integers, where $m \geq 2$ and $k \geq 6$ is even. If $m \mid U_k$, then $V_k S_k(m) \equiv U_k m \pmod{m^3}$.*

A prime p will be called *regular* if it does not divide any of the numerators U_r with even $r \leq p-3$, otherwise it is said to be *irregular*. The pairs (r, p) with $p \mid U_r$ and even $r \leq p-3$ are called *irregular pairs*. At a first glance this looks like a strange definition, but by celebrated work of Kummer [11] can be reformulated as: a prime p is irregular if and only if it divides the class number of $\mathbb{Q}(\zeta_p)$. The first few irregular primes are $37, 59, 67, 101, 103, 131, 149, \ldots$. It is known that there are infinitely many irregular primes, cf. Carlitz [5]. It is not known whether there are infinitely many regular primes. Let $\pi_\iota(x)$ denote the number of irregular primes $p \leq x$. Recently Luca et al. [12, Theorem 1] showed that

$$\pi_\iota(x) \geq (1 + o(1)) \frac{\log\log x}{\log\log\log x}, \quad x \to \infty.$$

Conjecturally, cf. Siegel [23], and in good agreement with numerical work, we should have

$$\pi_\iota(x) \sim \Big(1 - \frac{1}{\sqrt{e}}\Big)\pi(x) \approx 0.3935 \frac{x}{\log x}.$$

Let $N_\iota(x)$ denote the number of integers $n \leq x$ that are composed only of irregular primes. If we assume that

$$\pi_\iota(x) \sim \delta \frac{x}{\log x}, \quad 0 < \delta < 1, \tag{2.1}$$

then by Moree [18, Theorem 1] we have $N_\iota(x) \sim cx \log^{\delta-1} x$ as $x \to \infty$, with c a positive real constant. (Kummer conjectured that $\delta = 1/2$.) The latter result is of Wirsing type (cf. Schwarz and Spilker [22, pp. 65–76]).

For more results on Bernoulli numbers see, e.g., the book by Arakawa et al. [1].

3 The Kellner–Erdős–Moser Conjecture

In this section, we will use properties of Bernoulli numbers to study the non-trivial solutions of the equation $aS_k(m) = m^k$. This will then lead us to establish Theorem 3.11. As a bonus we will conclude that if $aS_k(m) = m^k$ has non-trivial solutions, then a must be either 1 or a product of irregular primes.

First assume that $m = 2$. Then $a = 2^k$. Next assume that $m = 3$. Then we must have $a(1 + 2^k) = 3^k$ and hence $a = 3^e$ for some $e \leq k$. It follows that $1 + 2^k = 3^{k-e}$. This Diophantine equation was already solved by the famous medieval astronomer Levi ben Gerson (1288–1344), alias Leo Hebraeus, who showed that 8 and 9 are the only consecutive integers in the sequence of powers of 2 and 3, see

Ribenboim [21, pp. 124–125]. This leads to the solutions $(e, k) \in \{(0, 1), (1, 3)\}$ and hence $(a, m, k) \in \{(1, 3, 1), (3, 3, 3)\}$. Now assume that $m \geq 4$ and k is odd. Then by Lemma 2.1 we find that $m(m-1)/2$ divides m^k, which is impossible. We infer that, to establish Conjecture 1.4, it is enough to establish the following conjecture.

Conjecture 3.1 *The set*

$$\mathcal{A} = \{a \geq 1 : aS_k(m) = m^k \text{ has a solution with } m \geq 4 \text{ and } k \text{ even}\}$$

is empty.

Lemma 3.2 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even. If p is a prime dividing m, then $(p-1) \nmid k$.*

Proof Assume that $p \mid m$ and $(p-1) \mid k$. Let $p^e \parallel m$ and $p^f \parallel a$, where $e \geq 1$, $f \geq 0$. Using Lemma 2.1 we find that $S_k(m) \equiv \frac{m}{p^e} S_k(p^e) \equiv -\frac{m}{p} \pmod{p^e}$. Hence $aS_k(m) \equiv -\frac{am}{p} \pmod{p^{e+f}}$, and so $m^k \equiv -\frac{am}{p} \pmod{p^{e+f}}$. Since $p^{e+f-1} \parallel \frac{am}{p}$, we deduce that $p^{e+f-1} \parallel m^k$, and thus $f = (k-1)e + 1 \geq k$. Then $a \geq p^k \geq 2^k$ and $aS_k(m) > 2^k(m-1)^k > m^k$, which contradicts the fact that $aS_k(m) = m^k$.

Corollary 3.3 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then we have* $\gcd(m, 6) = 1$.

Corollary 3.4 *If* $\gcd(a, 6) \neq 1$, *then $a \notin \mathcal{A}$.*

Lemma 3.5 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even. Suppose that a has no prime divisor p satisfying $p < 2^s$. Then $a \mid m^{\lceil k/s \rceil - 1}$.*

Proof Assume that $a \nmid m^{\lceil k/s \rceil - 1}$. Since each prime divisor of a divides m, there exists a prime p such that $p^{\lceil k/s \rceil} \mid a$. By assumption $p \geq 2^s$. Then $a \geq (2^s)^{\lceil k/s \rceil} \geq 2^k$ and $aS_k(m) \geq 2^k(m-1)^k > m^k$, which is a contradiction.

On combining the latter lemma and Corollary 3.4 we obtain the following result.

Corollary 3.6 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $a \mid m^{(k-2)/2}$.*

Lemma 3.7 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $m \mid U_k$.*

Proof Multiplying the Voronoi congruence by a and using the fact that $aS_k(m) = m^k$, we deduce that $V_k m^k \equiv U_k am \pmod{am^2}$. Since $m^2 \mid m^{(k+2)/2}$ and, by Corollary 3.6, $a \mid m^{(k-2)/2}$, we have $am^2 \mid U_k am$, that is $m \mid U_k$.

Corollary 3.8 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $k \geq 10$.*

Lemma 3.9 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $m^2 \mid U_k$.*

Proof By Corollary 3.8, $k \geq 10$. Using Lemma 2.6 instead of the Voronoi congruence and proceeding then by the same argument as in the proof of Lemma 3.7, we deduce that $am^3 \mid U_k am$, and so $m^2 \mid U_k$.

Since U_k is square-free for any even $k < 50$, we have

Corollary 3.10 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $k \geq 50$.*

In case $a = 1$ the next result is Lemma 10 of [19].

Theorem 3.11 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and even k. Let p be a prime dividing m. Then*

(a) *p is an irregular prime;*
(b) $k \not\equiv 0, 2, 4, 6, 8, 10, 14 \pmod{p-1}$*;*
(c) $\operatorname{ord}_p(B_k/k) \geq 2 \operatorname{ord}_p m \geq 2$*;*
(d) $k \equiv r \pmod{p-1}$ *for some irregular pair (r, p).*

Proof By Corollary 3.3 and Lemmas 3.2 and 3.7 we see that $p \geq 5$, $(p-1) \nmid k$ and $p \mid U_k$. If $p \nmid k$, then $\operatorname{ord}_p(B_k/k) > 0$ and p is irregular. Now assume that $p \mid k$, i.e., $\operatorname{ord}_p k \geq 1$. In view of Corollary 3.8 we have $k \geq 10$. Further

$$S_k(m) = B_k m + \frac{k(k-1)}{6} B_{k-2} m^3 + \sum_{j=4}^{k} \binom{k}{j} B_{k-j} \frac{m^{j+1}}{j+1}.$$

Hence

$$\frac{m^{k-1}}{ak} = \frac{B_k}{k} + \frac{k-1}{6} B_{k-2} m^2 + m^2 \sum_{j=4}^{k} \frac{(k-1)!}{(k-j)!} B_{k-j} \frac{m^{j-2}}{(j+1)!}. \tag{3.1}$$

By Lemma 2.2 we have $\operatorname{ord}_p V_{k-2} \leq 1$, and hence

$$\operatorname{ord}_p \left(\frac{k-1}{6} B_{k-2} m^2 \right) \geq 2 \operatorname{ord}_p m - \operatorname{ord}_p V_{k-2} \geq 1. \tag{3.2}$$

Further, for $j = 4, 5, \ldots, k$,

$$\operatorname{ord}_p \left(\frac{m^{j-2}}{(j+1)!} \right) = (j-2) \operatorname{ord}_p m - \frac{j+1-\sigma_p(j+1)}{p-1} \geq j - 2 - \frac{j}{4} \geq 1,$$

where $\sigma_p(j+1)$ denotes the sum of the digits of $j+1$ written in the base p. Therefore

$$\operatorname{ord}_p \left(m^2 \sum_{j=4}^{k} \frac{(k-1)!}{(k-j)!} B_{k-j} \frac{m^{j-2}}{(j+1)!} \right) \geq 2 \operatorname{ord}_p m \geq 2. \tag{3.3}$$

Note that

$$\operatorname{ord}_p\left(\frac{m^{k/2}}{k}\right) = \frac{k}{2}\operatorname{ord}_p m - \operatorname{ord}_p k \geq \frac{1}{2}p^{\operatorname{ord}_p k} - \operatorname{ord}_p k$$
$$> 2^{2\operatorname{ord}_p k - 1} - \operatorname{ord}_p k \geq \operatorname{ord}_p k \geq 1. \tag{3.4}$$

Using Corollary 3.6 we obtain

$$\operatorname{ord}_p\left(\frac{m^{(k-2)/2}}{a}\right) \geq 0. \tag{3.5}$$

It follows from (3.4) and (3.5) that

$$\operatorname{ord}_p\left(\frac{m^{k-1}}{ak}\right) = \operatorname{ord}_p\left(\frac{m^{(k-2)/2}}{a}\cdot\frac{m^{k/2}}{k}\right) \geq 1. \tag{3.6}$$

Combining (3.1)–(3.3) and (3.6), we deduce that $\operatorname{ord}_p(B_k/k) > 0$, and so p is irregular. This completes the proof of part (a). Part (b) is a consequence of part (a), Lemma 3.2 and the Kummer congruence. In the case $p \nmid k$, part (c) follows from Lemma 3.9. Now assume that $p \mid k$. By part (a), p is an irregular prime, and so $p \geq 37 > 2^5$. On combining Lemma 3.5 with $s = 5$ and Corollary 3.10, (3.5) is sharpened to

$$\operatorname{ord}_p\left(\frac{m^{(k-2)/2}}{a}\right) > 2\operatorname{ord}_p m.$$

Combining the latter estimate with (3.4) gives

$$\operatorname{ord}_p\left(\frac{m^{k-1}}{ak}\right) > 2\operatorname{ord}_p m. \tag{3.7}$$

Further, by part (b) and the von Staudt–Clausen theorem, $\operatorname{ord}_p V_{k-2} = 0$. Combining (3.1), (3.2), (3.3), and (3.7), we complete the proof of part (c). Part (d) is a direct consequence of part (c), the fact that $(p-1) \nmid k$, and the Kummer congruence.

Corollary 3.12 *If a has a regular prime divisor, then $a \notin \mathcal{A}$.*

Corollary 3.13 *Let p_1 and p_2 be distinct irregular prime divisors of a. Assume that for every pair (r_1, p_1), (r_2, p_2) of irregular pairs we have $\gcd(p_1 - 1, p_2 - 1) \nmid (r_1 - r_2)$. Then $a \notin \mathcal{A}$.*

`Example` Suppose that $37 \cdot 379 \mid a$. If $a \in \mathcal{A}$, then $aS_k(m) = m^k$ with $m \geq 4$ and k even and both 37 and 379 must divide m. There is one irregular pair $(32, 37)$ corresponding to 37 and two irregular pairs $(100, 379)$ and $(174, 379)$ corresponding to 379. By Theorem 3.11 (d), k must be a simultaneous solution

of the congruences $k \equiv 32 \pmod{36}$ and $k \equiv 100$ or $174 \pmod{378}$, which is impossible as $\gcd(36, 378) = 18$, $18 \nmid (32 - 100)$ and $18 \nmid (32 - 174)$. Hence $a \notin \mathcal{A}$.

4 Helpful Pairs

Helpful pairs will be used to show that certain ratios are forbidden (Sect. 5) and to show that certain numbers have to divide k (Sect. 7). In both cases one has to show that k is not in certain congruence classes. In order to show that a certain ratio is forbidden, we have to exclude *all* the congruence classes with an appropriate modulus. In order to show that a certain even number d divides k, we do this by excluding all the congruence classes $2i \pmod{d}$ for $1 \le i < d/2$. If $p \mid a$ is an irregular prime, $d = p - 1$, then by Theorem 3.11 we immediately exclude many congruence classes.

The exclusion of a congruence is achieved by a helpful pair and the procedure is described just after the proof of the crucial Lemma 4.4.

Definition 4.1 *For a positive integer a let us call a pair $(t, q)_a$ with q a prime and $2 \le t \le q - 3$ even to be* helpful *if $q \nmid a$ and $aS_t(c) \not\equiv c^t \pmod{q}$ for every integer c satisfying $1 \le c \le q - 1$. If q is an irregular prime, we require in addition that (t, q) should not be an irregular pair.*

Proposition 4.2 *Let $q \ge 5$ be a prime and a be a positive integer. Then $(2, q)_a$ is a helpful pair if and only if $\left(\frac{a^2+36a+36}{q}\right) = -1$.*

Proof Note that $B_2 = 1/6$ and hence $(2, q)$ cannot be an irregular pair. Since $S_2(c) = (2c^3 - 3c^2 + c)/6$, we see that $(2, q)_a$ is a helpful pair if and only if $q \nmid a$ and $a(2c^3 - 3c^2 + c) \not\equiv 6c^2 \pmod{q}$ for $c = 1, \ldots, q - 1$, that is, if and only if $a(2c^2 - 3c + 1) \not\equiv 6c \pmod{q}$ for $c = 0, \ldots, q - 1$, i.e., if and only if we have $\left(\frac{9(a+2)^2-8a^2}{q}\right) = \left(\frac{a^2+36a+36}{q}\right) = -1$.

Proposition 4.3 *Let $q \ge 7$ be a prime with $\left(\frac{31}{q}\right) = -1$. Then $(4, q)_{q-2}$ is a helpful pair.*

Proof From $\left(\frac{31}{q}\right) = -1$ we deduce that $6n^2 + 10n - 1 \not\equiv 0 \pmod{q}$ for $n = 1, \ldots, q - 1$. This implies that $30(q - 2)S_4(c) - 30c^4 \equiv -2c(6c^4 + 10c^2 - 1) \not\equiv 0 \pmod{q}$ for $c = 1, \ldots, q - 1$. Since $B_4 = -1/30$, $(4, q)$ is not an irregular pair. Thus $(4, q)_{q-2}$ is a helpful pair.

Lemma 4.4 *Let $2 \le t \le q - 3$ and q be a prime. If $(t, q)_a$ is a helpful pair and $aS_k(m) = m^k$ with k even, then we have $k \not\equiv t \pmod{q - 1}$.*

Proof Assume that $k \equiv t \pmod{q - 1}$. By Theorem 3.11 (d) we must have $q \nmid m$, for otherwise (t, q) is an irregular pair, contradicting the definition of a helpful pair. Thus we can write $m = m_0 q + b$ with $1 \le b \le q - 1$. By Lemma 2.1 we have

$q \mid S_t(q)$. We now find, modulo q, $S_k(m) \equiv S_t(m) \equiv m_0 S_t(q) + S_t(b) \equiv S_t(b)$. Thus if (1.3) is satisfied we must have $aS_t(b) \equiv b^t \pmod{q}$. By the definition of a helpful pair this is impossible.

Ruling Out Congruence Classes for k The helpful pairs give us a chance to rule out k that satisfy certain congruences of the form $k \equiv c \pmod{d}$ with $c \geq 2$ and d even. We first list all primes $q \geq 5$ such that $q-1$ divides d. Denote these primes by $q_1, \ldots, q_s$. Let t_i denote the least nonnegative integer congruent to c modulo $q_i - 1$. If one of the pairs $(t_i, q_i)_a$ is helpful, by Lemma 4.4 we have ruled out $k \equiv c \pmod{d}$. If this does not work, we multiply d by an integer $\ell \geq 2$ (*the lifting factor*). Our original congruence is now replaced by ℓ congruences, $k \equiv c + jd \pmod{\ell d}$, $0 \leq j < \ell$. For each of these congruences we now continue as before. In certain cases we find that each of the lifted congruences is ruled out by a helpful pair and then we are done. This situation is described in Proposition 4.5 below. If not all of the lifted congruences are excluded by helpful pairs, we can lift the bad congruences still further. The above procedure is not systematic and each stage the danger lurks that we get too many congruence classes we cannot exclude anymore.

Proposition 4.5 *Let p be an irregular prime dividing a. Assume that for every irregular pair (r,p) there exists a positive integer ℓ_r such that for every $j = 0, 1, \ldots, \ell_r - 1$ there is a helpful pair $(t_j, q_j)_a$ with $(q_j - 1) \mid \ell_r(p-1)$ and $t_j \equiv r + j(p-1) \pmod{q_j - 1}$. Then $a \notin \mathcal{A}$.*

Proof Since p must divide m, Theorem 3.11 (d) yields $k \equiv r \pmod{p-1}$ for some irregular pair (r,p). Hence there exists $j \in \{0, 1, \ldots, \ell_r - 1\}$ such that $k \equiv r + j(p-1) \pmod{\ell_r(p-1)}$. Then we have $k \equiv t_j \pmod{q_j - 1}$ for the helpful pair $(t_j, q_j)_a$, which contradicts Lemma 4.4.

Corollary 4.6 *Under the conditions of Proposition 4.5, we have $ab \notin \mathcal{A}$ for any positive integer $b \equiv 1 \pmod{Q}$, where Q denotes the least common multiple of all components q_j of helpful pairs constructed for all irregular pairs (r,p) corresponding to p.*

5 Excluding a Given Ratio ρ

Let $\rho \geq 3$. Write $a = \rho - 1$. If a has no regular prime divisor, the only way we know to exclude ρ is by using helpful pairs or invoking Corollary 3.13. We demonstrate this with two examples (an example of the usage of Corollary 3.13 we already gave immediately following the statement of Corollary 3.13).

`Easy example:` $a = 673$.

There are two irregular pairs $(408, 673)$ and $(502, 673)$ corresponding to 673. Theorem 3.11 (d) yields $k \equiv 408$ or $502 \pmod{672}$. If $k \equiv 408 \pmod{672}$, then $k \equiv 8 \pmod{16}$. The latter is impossible since $(8, 17)_{10}$ is a helpful pair by Table 2

in Appendix. If $k \equiv 502 \pmod{672}$, then $k \equiv 2 \pmod 4$, which is impossible as $(2, 5)_3$ is a helpful pair by Table 2 in Appendix.

`Difficult example:` $a = 653$.

There is one irregular pair $(48, 653)$ corresponding to 653, and so $k \equiv 48 \pmod{652}$. We have $652 = 2^2 \cdot 163$. There are no helpful pairs $(48, q)$ with $(q - 1) \mid 652$. So we have to use a lifting factor ℓ. It turns out that $\ell = 4$ is a useful factor. So that is why we use it in the first step.

Step 1. We have $k \equiv 48$ or 700 or 1352 or 2004 $\pmod{2608}$. The case $k \equiv 48 \pmod{2608}$ is impossible, since $(48, 2609)_{653}$ is a helpful pair. If $k \equiv 700$ or 1352 $\pmod{2608}$, then $k \equiv 8$ or 12 $\pmod{16}$, which is impossible as $(8, 17)_7$ and $(12, 17)_7$ are helpful pairs. Thus $k \equiv 2004 \pmod{2608}$.

Step 2. We have $k \equiv 2004$ or 4612 or 7220 or 9828 or 12436 $\pmod{13040}$. If $k \equiv 4612$ or 7220 or 9828 $\pmod{13040}$, then $k \equiv 12$ or 20 or 28 $\pmod{40}$. From the fact that $(12, 41)_{38}$, $(20, 41)_{38}$ and $(28, 41)_{38}$ are helpful pairs we deduce that the latter congruence is impossible. Hence $k \equiv 2004$ or 12436 $\pmod{13040}$.

Step 3. We have $k \equiv 2004$ or 12436 or 15044 or 25476 or 28084 or 38516 $\pmod{39120}$. If $k \equiv 15044$ or 28084 $\pmod{39120}$, then $k \equiv 4$ or 14 $\pmod{30}$, which is impossible as $(4, 31)_2$ and $(14, 31)_2$ are helpful pairs. If $k \equiv 2004$ or 25476 $\pmod{39120}$, then $k \equiv 24$ or 36 $\pmod{60}$. The latter is impossible, since $(24, 61)_{43}$ and $(36, 61)_{43}$ are helpful pairs. The case $k \equiv 12436 \pmod{39120}$ implies $k \equiv 196 \pmod{240}$, which is impossible as $(196, 241)_{171}$ is a helpful pair. The remaining case $k \equiv 38516 \pmod{39120}$ is also impossible, since in this case $k \equiv 9176 \pmod{9780}$ and $(9176, 9781)_{653}$ is a helpful pair.

`Remark` Using helpful pairs, we can find some infinite families of forbidden ratios. For example, let $\rho = 37^s + 1$ for some positive integer s. The prime 37 is irregular and $(32, 37)$ an irregular pair. If $37^s S_k(m) = m^k$ with k even then, by Theorem 3.11 (d), we have $k \equiv 32 \pmod{36}$. This implies that $k \equiv 8 \pmod{12}$. Since $(8, 13)_{37^s}$ is a helpful pair if and only if $37^s \equiv 1$ or 2 or 6 or 8 or 11 $\pmod{13}$ (see Table 2 in Appendix), we deduce that $\rho = 37^s + 1$ is a forbidden ratio for any $s \equiv 0$ or 1 or 7 or 9 or 11 $\pmod{12}$.

6 Bad Ratios

Table 3 in Appendix gives a list of ratios we excluded and the helpful pairs used to do so. The attentive reader will notice that various ratios ρ are apparently bad and difficult to exclude. These are related to $a = \rho - 1$ that are of the form $(2p + 1)^s$ with p a *Sophie Germain prime*. Recall that a prime p is said to be a *Sophie Germain prime* if also $2p + 1$ is a prime. Heuristics suggests that there ought to be infinitely many Sophie Germain primes such that $2p + 1$ is an irregular prime.

Conjecture 6.1 *There are infinitely many primes p such that $2p+1$ is an irregular prime.*

Let p be a prime such that $2p+1$ is an irregular prime and let $(r, 2p+1)$ be an irregular pair. In case we want to rule out $k \equiv r \pmod{2p}$ we are in bad shape to start with. We are directly forced here to use a lifting factor $\ell \geq 2$ (as the list of primes $5 \leq q < 2p+1$ with $(q-1) \mid 2p$ is empty here). The next result shows that we are in even worse shape, since helpful pairs with primes $q = 2pu+1 > 6p$ have to be used.

Proposition 6.2 *Let p be a prime such that $2p+1$ is an irregular prime dividing a and let $(r, 2p+1)$ be an irregular pair. Let ℓ be a positive integer with $p \nmid \ell$, let $q_0, q_1, \ldots, q_{\ell-1}$ be odd primes with $(q_j - 1) \mid 2\ell$ (not necessarily distinct) and let $t_0, t_1, \ldots, t_{\ell-1}$ be positive integers satisfying the conditions $t_j \equiv r + 2pj \pmod{q_j - 1}$, $0 \leq j \leq \ell - 1$. Then at least one of the pairs $(t_0, q_0)_a, (t_1, q_1)_a, \ldots, (t_{\ell-1}, q_{\ell-1})_a$ is not a helpful pair.*

Proof Since r is even and $p \nmid \ell$, there exists a j with $0 \leq j \leq \ell - 1$ such that $pj \equiv -r/2 \pmod{\ell}$. Hence $2\ell \mid (r + 2pj)$. This implies that $(q_j - 1) \mid t_j$, and so $(t_j, q_j)_a$ is not a helpful pair.

In case we are not able to exclude such a bad ratio, we might try at least to show that the k of a solution has to be highly divisible. In the next section we demonstrate this for the bad ratio 6780.

7 Divisibility of k

In this section, we consider the case $a = 6779 = 2 \cdot 3389 + 1$ and show that for a non-trivial solution k is divisible by a large number. We will present a heuristic argument here why we think that for this a there are no solutions. We expect that a similar reasoning might work for other values of a as well, once one can establish that a smallish number like 120 divides k.

We start by discussing a baby example.

Proposition 7.1

(a) *If* $a \equiv 1$ *or* 2 *or* $3 \pmod 5$, *then* $4 \mid k$.
(b) *If* $a \equiv 1$ *or* 3 *or* $5 \pmod 7$, *then* $6 \mid k$.
(c) *If* $a \equiv 6$ *or* $7 \pmod{11}$, *then* $10 \mid k$.
(d) *If* $a \equiv 2$ *or* 8 *or* $11 \pmod{13}$, *then* $12 \mid k$.
(e) *If* $a \equiv 1$ *or* $6 \pmod{13}$, *then* $6 \mid k$.
(f) *If* $a \equiv 1$ *or* $5 \pmod{11}$ *and* $a \equiv 15 \pmod{31}$, *then* $10 \mid k$.

Proof If, e.g., $a \equiv 2 \pmod{13}$, we see from Table 2 in Appendix that the pairs $(2, 13)_a$, $(4, 13)_a$, $(6, 13)_a$, $(8, 13)_a$ and $(10, 13)_a$ are all helpful. The final assertion follows from glancing at an extended version of Table 2 in Appendix.

Now let us consider a more serious example, with $\rho = 6780$ a bad ratio.

Proposition 7.2 *If* $6779S_k(m) = m^k$, *then* $2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \mid k$.

Proof We start with the congruence $k \equiv 3994 \pmod{6778}$, which is a consequence of Theorem 3.11 (d) and the fact that there is only one irregular pair $(3994, 6779)$ corresponding to 6779.

Step 1. We have $k \equiv 3994$ or 10772 or $17550 \pmod{20334}$. If $k \equiv 3994$ or $10772 \pmod{20334}$, then $k \equiv 2$ or $4 \pmod 6$, which is impossible as $(2, 7)_3$ and $(4, 7)_3$ are helpful pairs. Hence $k \equiv 17550 \pmod{20334}$ and $2 \cdot 3 \mid k$.

Step 2. We have $k \equiv 17550$ or 37884 or $58218 \pmod{61002}$. The case $k \equiv 58218 \pmod{61002}$ is impossible, since in this case $k \equiv 6 \pmod{18}$ and $(6, 19)_{15}$ is a helpful pair. Hence $k \equiv 17550$ or $37884 \pmod{61002}$.

Step 3. We have $k \equiv 17550$ or 37884 or 78552 or $98886 \pmod{122004}$. If $k \equiv 17550$ or $98886 \pmod{122004}$, then $k \equiv 18$ or $30 \pmod{36}$, which is impossible as $(18, 37)_8$ and $(30, 37)_8$ are helpful pairs. Hence $k \equiv 37884$ or $78552 \pmod{122004}$.

Step 4. We have $k \equiv 37884$ or 78552 or 159888 or $200556 \pmod{244008}$. If $k \equiv 37884$ or 159888 or $200556 \pmod{244008}$, then $k \equiv 12$ or 36 or $48 \pmod{72}$, which is impossible as $(12, 73)_{63}$, $(36, 73)_{63}$ and $(48, 73)_{63}$ are helpful pairs. Hence $k \equiv 78552 \pmod{244008}$ and $2^3 \cdot 3^2 \mid k$.

Step 5. We have $k \equiv 78552$ or $322560 \pmod{488016}$. In the case $k \equiv 78552 \pmod{488016}$ we have $k \equiv 8 \pmod{16}$, which is impossible as $(8, 17)_{13}$ is a helpful pair. Hence $k \equiv 322560 \pmod{488016}$ and $2^4 \cdot 3^2 \mid k$.

Step 6. We have $k \equiv 322560$ or $810576 \pmod{976032}$. The case $k \equiv 810576 \pmod{976032}$ is impossible, since in this case $k \equiv 48 \pmod{96}$ and $(48, 97)_{86}$ is a helpful pair. Hence $k \equiv 322560 \pmod{976032}$ and $2^5 \cdot 3^2 \mid k$.

Step 7. We have $k \equiv 322560$ or $1298592 \pmod{1952064}$. In the case $k \equiv 1298592 \pmod{1952064}$ we have $k \equiv 288 \pmod{576}$. The latter is impossible, since $(288, 577)_{432}$ is a helpful pair. Hence $k \equiv 322560 \pmod{1952064}$ and $2^6 \cdot 3^2 \mid k$.

Step 8. We have $k \equiv 322560$ or 2274624 or $4226688 \pmod{5856192}$. The case $k \equiv 322560 \pmod{5856192}$ is impossible, since in this case $k \equiv 288 \pmod{432}$ and $(288, 433)_{284}$ is a helpful pair. In the case $k \equiv 2274624 \pmod{5856192}$ we have $k \equiv 36 \pmod{108}$, which is impossible as $(36, 109)_{21}$ is a helpful pair. Hence $k \equiv 4226688 \pmod{5856192}$ and $2^6 \cdot 3^3 \mid k$.

Step 9. We have $k \equiv 4226688$ or 10082880 or 15939072 or 21795264 or $27651456 \pmod{29280960}$. If $k \equiv 15939072$ or $27651456 \pmod{29280960}$, then $k \equiv 6$ or $12 \pmod{30}$, which is impossible as $(6, 31)_{21}$ and $(12, 31)_{21}$ are helpful pairs. In the case $k \equiv 21795264 \pmod{29280960}$ we have $k \equiv 24 \pmod{60}$, which is impossible since $(24, 61)_8$ is a helpful pair. The case $k \equiv 4226688 \pmod{29280960}$ is also impossible, since in this case $k \equiv 108 \pmod{180}$ and $(108, 181)_{82}$ is a helpful pair. Hence $k \equiv 10082880 \pmod{29280960}$ and $2^6 \cdot 3^3 \cdot 5 \mid k$.

Step 10. We have $k \equiv 10082880 + 29280960j \pmod{204966720}$ for some $j \in \{0, 1, \ldots, 6\}$. If $j \in \{0, 1, 3, 6\}$, then $k \equiv 8$ or 12 or 16 or 24 (mod 28), which is impossible as $(8, 29)_{22}$, $(12, 29)_{22}$, $(16, 29)_{22}$ and $(24, 29)_{22}$ are helpful pairs. If $j = 4$ or 5, then we have $k \equiv 6$ or 18 (mod 42). The latter is impossible, since $(6, 43)_{28}$ and $(18, 43)_{28}$ are helpful pairs. Hence $k \equiv 68644800 \pmod{204966720}$ and $2^6 \cdot 3^3 \cdot 5 \cdot 7 \mid k$.

Step 11. We have $k \equiv 68644800 + 204966720j \pmod{1024833600}$ for some $j \in \{0, 1, 2, 3, 4\}$. If $j \in \{1, 2, 3\}$, then $k \equiv 20$ or 40 or 60 (mod 100), which is impossible as $(20, 101)_{12}$, $(40, 101)_{12}$ and $(60, 101)_{12}$ are helpful pairs. The case $j = 4$ is also impossible, since in this case $k \equiv 3780 \pmod{6300}$ and $(3780, 6301)_{478}$ is a helpful pair. Hence $k \equiv 68644800 \pmod{1024833600}$ and $2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \mid k$.

Step 12. We have $k \equiv 68644800 + 1024833600j \pmod{11273169600}$ for some $j \in \{0, 1, \ldots, 10\}$. If $j \in \{0, 2, 3, 6, 8\}$, then $k \equiv 2$ or 4 or 12 or 18 or 20 (mod 22), which is impossible as $(2, 23)_{17}$, $(4, 23)_{17}$, $(12, 23)_{17}$, $(18, 23)_{17}$ and $(20, 23)_{17}$ are helpful pairs. If $j \in \{1, 5, 7\}$, then $k \equiv 30$ or 36 or 54 (mod 66), which is impossible since $(30, 67)_{12}$, $(36, 67)_{12}$ and $(54, 67)_{12}$ are helpful pairs. In the case $j = 10$ we have $k \equiv 16 \pmod{88}$, which is impossible as $(16, 89)_{15}$ is a helpful pair. The case $j = 9$ is also impossible, since in this case $k \equiv 160 \pmod{352}$ and $(160, 353)_{72}$ is a helpful pair. Hence $k \equiv 4167979200 \pmod{11273169600}$ and $2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \mid k$.

Step 13. We have $k \equiv 4167979200 + 11273169600j \pmod{146551204800}$ for some $j \in \{0, 1, \ldots, 12\}$. If $j \in \{1, 3, 4, 5, 7, 8, 10\}$, then $k \equiv 12$ or 20 or 24 or 28 or 36 or 40 or 48 (mod 52), which is impossible as $(12, 53)_{48}$, $(20, 53)_{48}$, $(24, 53)_{48}$, $(28, 53)_{48}$, $(36, 53)_{48}$, $(40, 53)_{48}$ and $(48, 53)_{48}$ are helpful pairs. If $j = 2$ or 12, then $k \equiv 30$ or 42 (mod 78), which is impossible, since $(30, 79)_{64}$ and $(42, 79)_{64}$ are helpful pairs. If $j = 0$ or 6, then $k \equiv 60$ or 110 (mod 130), which is impossible as $(60, 131)_{98}$ and $(110, 131)_{98}$ are helpful pairs. The case $j = 9$ is also impossible, since in this case $k \equiv 96 \pmod{156}$ and $(96, 157)_{28}$ is a helpful pair. Hence $k \equiv 128172844800 \pmod{146551204800}$ and $2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \mid k$.

It seems that the type of argument used in the proof of Proposition 7.2 can be continued to deduce that more and more small prime factors must divide k. Given a prime $q \geq 5$ and $2 \leq t \leq q - 3$ even, one would heuristically expect that $(t, q)_a$ is helpful with probability $(1 - 1/q)^{q-1}$ which tends to $1/e$, on assuming that the values $S_t(c)$ are randomly distributed modulo q. The numerical data obtained so far turn out to be consistent with this.

For the original Erdős–Moser equation it is known (cf. [8, 19]) that $N \mid k$ with

$$N = 2^8 \cdot 3^5 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdots 997 > 5.7462 \cdot 10^{427}.$$

A heuristic argument can be given suggesting that if, say $L_v := \mathrm{lcm}(1, 2, \ldots, v)$ divides k, with tremendously high likelihood we can infer that L_w divides k, where w is the smallest prime not dividing L_v. It is already enough to have $v \geq 11$ here. To

deduce that k is divisible by say 24 might be delicate, but once one has $L_v \mid k$ say, there is an explosion of further helpful pairs one can use to establish divisibility of k by an even larger integer. To add the first prime w not dividing L_v, one needs to have only a number of helpful pairs that is roughly linear in v, whereas an exponential number (in v) is available. However, the required computation time goes sharply up with increasing w.

This result gives a lower bound of 10^{427} for k, which is modest in comparison with the lower bound obtained by Moser. However, as argued by Gallot et al. [6], a result of the form $N \mid k$ leads to an expected lower bound $m > 10^{257N}$. For the Kellner–Erdős–Moser equation we likewise expect a result of the form $N \mid k$ to lead to a lower bound for m that is exponential in N.

Unfortunately, the authors are not aware of any systematic approach that would allow one to prove a result of the type that if $aS_k(m) = m^k$, then $120 \mid k$, for every $a \geq 1$. Some preliminary work on this for the equation $S_k(m) = am^k$ was done by the second author's intern Muriel Lang in 2009.

8 Lower Bound for m

The aim of this section is to establish Theorem 8.4. The proof rests on Lemmas 8.1 and 8.3.

Lemma 8.1 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even. Then $m-1$ and $2m-1$ are square-free, and if p is a prime divisor of $(m-1)(2m-1)$, then $(p-1) \mid k$.*

Proof Since

$$S_k(m-1) = S_k(m) - (m-1)^k \equiv S_k(m) \pmod{m-1},$$

Lemma 2.1 yields

$$a \sum_{\substack{p \mid (m-1) \\ (p-1) \mid k}} \frac{m-1}{p} + m^k \equiv 0 \pmod{a(m-1)}. \tag{8.1}$$

Note that if $p \mid (m-1)$ and $(p-1) \nmid k$, then $p \mid m$, a contradiction that shows that $p \mid (m-1)$ implies $(p-1) \mid k$. If $p^2 \mid (m-1)$, it follows again that $p \mid m$, a contradiction that shows that $m-1$ is square-free.

Note that

$$S_k(2m-1) = \sum_{j=1}^{m-1} (j^k + (2m-1-j)^k) \equiv 2S_k(m) \pmod{2m-1}.$$

Then, again by Lemma 2.1,

$$a \sum_{\substack{p|(2m-1)\\(p-1)|k}} \frac{2m-1}{p} + 2m^k \equiv 0 \pmod{a(2m-1)}, \tag{8.2}$$

from which we deduce that $2m-1$ is square-free and each prime p dividing $2m-1$ satisfies $(p-1) \mid k$.

Corollary 8.2 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even, then $m \equiv 3 \pmod 4$.*

Lemma 8.3 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even and let p be a prime divisor of $(m+1)(2m+1)$. If $(p-1) \mid k$ then $\mathrm{ord}_p((m+1)(2m+1)) = \mathrm{ord}_p(a+1)+1$, otherwise $\mathrm{ord}_p((m+1)(2m+1)) \leq \mathrm{ord}_p(a+1)$.*

Proof Observe that $aS_k(m+1) = (a+1)m^k$. Invoking Lemma 2.1, we obtain

$$a \sum_{\substack{p|(m+1)\\(p-1)|k}} \frac{m+1}{p} + (a+1)m^k \equiv 0 \pmod{a(m+1)}. \tag{8.3}$$

Since $p \mid a$ implies $p \mid m$ it follows that $\gcd(a, m+1) = 1$. Thus

$$\begin{aligned} &\mathrm{ord}_p(m+1) = \mathrm{ord}_p(a+1) + 1 && \text{if } p \mid (m+1) \text{ and } (p-1) \mid k,\\ &\mathrm{ord}_p(m+1) \leq \mathrm{ord}_p(a+1) && \text{if } p \mid (m+1) \text{ and } (p-1) \nmid k. \end{aligned}$$

Further, from

$$aS_k(2m+1) = a\sum_{j=1}^{m}(j^k + (2m+1-j)^k) \equiv 2aS_k(m+1) \equiv 2(a+1)m^k \pmod{a(2m+1)}$$

we deduce that

$$a \sum_{\substack{p|(2m+1)\\(p-1)|k}} \frac{2m+1}{p} + 2(a+1)m^k \equiv 0 \pmod{a(2m+1)}, \tag{8.4}$$

and so

$$\begin{aligned} &\mathrm{ord}_p(2m+1) = \mathrm{ord}_p(a+1) + 1 && \text{if } p \mid (2m+1) \text{ and } (p-1) \mid k,\\ &\mathrm{ord}_p(2m+1) \leq \mathrm{ord}_p(a+1) && \text{if } p \mid (2m+1) \text{ and } (p-1) \nmid k. \end{aligned}$$

Since $m+1$ and $2m+1$ are coprime, the asserted result follows.

Part (g) below arose in collaboration with Jan Büthe and we only provide a sketch of the proof here. We remark that if the condition $m \equiv 1 \pmod{30}$ is replaced by

$$\sum_{p|(m-1)} \frac{1}{p} + \frac{1}{a} > 1,$$

[cf. Eq. (8.11)] the same conclusion holds true.

Theorem 8.4 *Assume that $a > 1$ is square-free and that $aS_k(m) = m^k$ with $m \geq 4$ and k even. Put $a_1 = \gcd(a+1, m+1)$ and $a_2 = \gcd(a+1, 2m+1)$. Put*

$$M = \frac{(m^2-1)(4m^2-1)}{6a_1a_2}.$$

Then

(a) $m > a$;
(b) $m-1$, $2m-1$, $(m+1)/a_1$, *and* $(2m+1)/a_2$ *are all square-free;*
(c) *if p divides at least one of the above four integers, then $(p-1) \mid k$;*
(d) $m > 3.4429 \cdot 10^{82}$;
(e) *the number M is square-free and has at least* 139 *prime factors;*
(f) *if $m \equiv 1 \pmod 3$, then $m > 1.485 \cdot 10^{9321155}$ and the number M has at least* 4990906 *prime factors;*
(g) *if $m \equiv 1 \pmod{30}$, then $m > 10^{4 \cdot 10^{20}}$ and the number M has at least* 75760524354901799895 *prime factors.*

Proof As a is square-free, we have $a \mid m$, and so $m \geq a$. If $m = a$, then (8.3) yields

$$\sum_{\substack{p|(m+1) \\ (p-1)|k}} \frac{1}{p} \equiv 0 \pmod 1.$$

Since the sum of reciprocals of distinct primes can never be a positive integer, we must have

$$\sum_{\substack{p|(m+1) \\ (p-1)|k}} \frac{1}{p} = 0,$$

which contradicts the fact that $2 \mid (m+1)$. Parts (b) and (c) are direct consequences of Lemmas 8.1 and 8.3. Further, using Lemma 8.3, parts (b) and (c) and the facts that $a \mid m$ and $\gcd(a, m-1) = \gcd(a, 2m-1) = \gcd(a, m+1) = \gcd(a, 2m+1) = 1$, we find that

$$m^k \equiv m \pmod{a(m-1)},$$
$$2m^k \equiv 4m \pmod{a(2m-1)},$$

$$(a+1)m^k \equiv a+1+(a-1)(m+1) \pmod{a(m+1)},$$
$$2(a+1)m^k \equiv 2(a+1)+(a-2)(2m+1) \pmod{a(2m+1)}.$$

Here we will only provide details for the latter congruence, which is the most complicated one to establish. Since a and $2m+1$ are coprime, it suffices by the Chinese remainder theorem to establish the congruence modulo a and modulo $2m+1$. Since $a \mid m$ the congruence trivially holds modulo a.

Now suppose that $p \mid (2m+1)$.

`First case:` $(p-1) \mid k$.

By Lemma 8.3 we have $\mathrm{ord}_p(2m+1) = \mathrm{ord}_p(a+1)+1$ and it suffices to show that $m^k \equiv 1 \pmod{p}$. This is true by Euler's theorem.

`Second case:` $(p-1) \nmid k$.

Here we use that, by Lemma 8.3 again, $\mathrm{ord}_p(2m+1) \leq \mathrm{ord}_p(a+1)$ to see that the congruence holds.

We can rewrite the congruences (8.1)–(8.4) as

$$\sum_{p \mid (m-1)} \frac{1}{p} + \frac{m}{a(m-1)} \equiv 0 \pmod{1}, \tag{8.5}$$

$$\sum_{p \mid (2m-1)} \frac{1}{p} + \frac{4m}{a(2m-1)} \equiv 0 \pmod{1}, \tag{8.6}$$

$$\sum_{p \mid \frac{m+1}{a_1}} \frac{1}{p} + \frac{a+1+(a-1)(m+1)}{a(m+1)} \equiv 0 \pmod{1}, \tag{8.7}$$

$$\sum_{p \mid \frac{2m+1}{a_2}} \frac{1}{p} + \frac{2(a+1)+(a-2)(2m+1)}{a(2m+1)} \equiv 0 \pmod{1}. \tag{8.8}$$

By Corollary 8.2, the assumption that k is even and Lemma 8.3, we see that $(m+1)/a_1$ is even. Now noting that $a \geq 37$ (by Corollary 3.12 and the fact that 37 is the first irregular prime), we have

$$\sum_{p \mid \frac{m+1}{a_1}} \frac{1}{p} + \frac{a+1+(a-1)(m+1)}{a(m+1)} \geq \frac{1}{2} + \frac{a+1+a(m+1)}{a(m+1)} - \frac{1}{a} > 1.$$

Therefore, if we add the left-hand sides of (8.5)–(8.8), we get an integer, at least 5. No prime $p > 3$ can divide more than one of the integers $m-1$, $2m-1$, $(m+1)/a_1$, and $(2m+1)/a_2$, and 2 and 3 divide precisely two of these integers. Hence $M =$

$(m^2-1)(4m^2-1)/(6a_1a_2)$ is square-free and

$$\sum_{p|M}\frac{1}{p}+\frac{1}{a(m-1)}+\frac{2}{a(2m-1)}+\frac{a+1}{a(m+1)}+\frac{2(a+1)}{a(2m+1)}$$
$$\geq 3-\frac{1}{2}-\frac{1}{3}=2\frac{1}{6}. \tag{8.9}$$

Since $a \mid m$, $m > a \geq 37$ and each prime divisor of m is irregular, we have $m \geq 37^2$. A simple computation shows that (8.5) is never satisfied for $a \geq 37$ and $m = 37^2$. Since 59 is the second irregular prime, it follows that $m \geq 37 \cdot 59$. On noting that the four fractions above are decreasing functions in both a and m, we find on substituting $a = 37$ and $m = 37 \cdot 59$ that $\sum_{p|M}\frac{1}{p} > \alpha$, with $\alpha = 2.1657$. Note that if

$$\sum_{p\leq x}\frac{1}{p} < \alpha, \tag{8.10}$$

then $m^4/3 > M > \prod_{p\leq x} p$ (note that $a_1 \geq 2$ and hence $M < m^4/3$). One computes (using a computer algebra package) the largest prime p_s such that $\sum_{p_j\leq p_s}\frac{1}{p_j} < 2\frac{1}{6}$, with $p_1, p_2, \ldots$ the consecutive primes. Here one finds that $s = 139$ and

$$\sum_{j=1}^{139}\frac{1}{p_j} < 2.16566 < \alpha < \sum_{p|M}\frac{1}{p}.$$

Thus

$$m > \left(3\prod_{p\leq p_{139}} p\right)^{1/4} > 3.4429 \cdot 10^{82}.$$

Now assume that $m \equiv 1 \pmod 3$. Then $3 \mid (2m+1)/a_1$ by Lemma 8.3, and so

$$\sum_{p|\frac{2m+1}{a_2}}\frac{1}{p}+\frac{2(a+1)+(a-2)(2m+1)}{a(2m+1)} \geq \frac{1}{3}+\frac{2(a+1)+a(2m+1)}{a(2m+1)}-\frac{1}{a/2} > 1.$$

Hence in this case, $2\frac{1}{6}$ in (8.9) can be replaced by $3\frac{1}{6}$. This α occurs in the work of Moser and here it is known that $s = 4990906$, leading to $m > 1.485 \cdot 10^{9321155}$ (cf. [4, 16]).

Finally, assume that $m \equiv 1 \pmod{30}$. Then

$$\sum_{p|(m-1)}\frac{1}{p}+\frac{m}{a(m-1)} > \frac{1}{2}+\frac{1}{3}+\frac{1}{5} > 1, \tag{8.11}$$

and we have the inequality (8.9) with $2\frac{1}{6}$ replaced by $4\frac{1}{6}$. In this case the largest prime p_s such that $\sum_{p\le p_s}\frac{1}{p} < 4\frac{1}{6}$ can no longer be determined by direct computation and more sophisticated methods are needed, cf. [2].

`Remark` Note that in the proof we only used that $a \ge 37$. This has as a consequence that the proof only depends on the first assertion in Theorem 1.5.

9 Proofs of the New Results Announced in the Introduction

It remains to establish Theorem 1.5, Theorem 1.6 and Proposition 1.7.

Proof of Theorem 1.5 The first restriction on a arises on invoking Corollary 3.12. In order to obtain the second restriction we have to write down all integers $a \le 1500$ that are composed only of irregular primes. These are listed in Table 3 in Appendix. Each of these can be excluded as is shown for two examples in Sect. 5. This exclusion process for each a can be reconstructed using Table 3 in Appendix.

To prove Theorem 1.6 we need the following result, which shows that m and k are of comparable size.

Lemma 9.1 *Suppose that* $aS_k(m) = m^k$. *Then* $k+1 < am < (a+1)(k+1)$.

Proof We have

$$S_k(m) \le \int_1^m x^k \mathrm{d}x \le S_k(m+1) - 1.$$

Hence

$$m^k = aS_k(m) \le a\int_1^m x^k \mathrm{d}x = \frac{a(m^{k+1}-1)}{k+1} < \frac{am^{k+1}}{k+1},$$

and so $am > k+1$. Further,

$$(a+1)m^k = aS_k(m+1) \ge a\left(1 + \int_1^m x^k \mathrm{d}x\right) = \frac{a(m^{k+1}+k)}{k+1} > \frac{am^{k+1}}{k+1},$$

that is $am < (a+1)(k+1)$.

Proof of Theorem 1.6 The lower bound on m is a consequence of Theorem 8.4, part (d). On invoking Lemma 9.1 with $a \ge 1501$ the result follows.

Proof of Proposition 1.7 Let (m, k) be a solution of (1.3). Observe that

$$\frac{S_j(m)}{m^j} = \left(\frac{1}{m}\right)^j + \left(\frac{2}{m}\right)^j + \cdots + \left(\frac{m-1}{m}\right)^j > \frac{S_{j+1}(m)}{m^{j+1}},$$

and so

$$\begin{aligned} aS_j(m) - m^j &> 0 \qquad \text{if } j < k, \\ aS_j(m) - m^j &< 0 \qquad \text{if } j > k. \end{aligned} \tag{9.1}$$

This shows that for every m, there is at most one k.

Now assume that there exists a positive integer n such that $aS_k(m+n) = (m+n)^k$. Then $k > 1$. Since

$$S_k(m+n) = S_k(n) + \sum_{j=0}^{m-1}(n+j)^k = S_k(n) + mn^k + \sum_{j=1}^{k}\binom{k}{j}n^{k-j}S_j(m),$$

we have

$$(m+n)^k = \sum_{j=0}^{k}\binom{k}{j}m^j n^{k-j} = aS_k(n) + amn^k + a\sum_{j=1}^{k}\binom{k}{j}n^{k-j}S_j(m),$$

or, equivalently,

$$n^k = aS_k(n) + amn^k + \sum_{j=1}^{k-1}\binom{k}{j}n^{k-j}(aS_j(m) - m^j).$$

In view of (9.1), the last equality cannot hold. Thus we see that, for every k, there is at most one m.

`Remark` Using the same type of argument, we can prove the following: if (m_1, k_1) and (m_2, k_2) are two distinct solutions of $aS_k(m) = m^k$, then either $m_1 > m_2, k_1 > k_2$ or $m_1 < m_2, k_1 < k_2$.

10 Other Properties of Kellner–Erdős–Moser Solutions

There are many restrictions known that a solution of the Erdős–Moser equation has to satisfy. We expect that most of these have an analogue for the Kellner–Erdős–Moser equation as well. We present an example.

Theorem 10.1 *Suppose that $aS_k(m) = m^k$ with $m \geq 4$ and k even. We have*

$$\operatorname{ord}_2(a(m-1)-2) \begin{cases} = 3 + \operatorname{ord}_2 k & \text{if } a \equiv 1 \pmod 4, \\ \geq 4 + \operatorname{ord}_2 k & \text{if } a \equiv 3 \pmod 4. \end{cases}$$

For $a = 1$ this was first established in Moree et al. [19, Lemma 12] using Bernoulli numbers. A much more elementary proof also dealing with solutions of the equation $S_k(m) = am^k$ for integers a was given later by the second author [15].

Our proof of Theorem 10.1 makes use of the following lemma.

Lemma 10.2 *Let k and m be positive integers where $k \geq 6$ is even. Then*

$$S_k(m) \equiv \begin{cases} \left[\frac{m}{2}\right] + 2^{2+\operatorname{ord}_2 k} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } \left[\frac{m}{2}\right] \equiv 2 \pmod 4, \\ \left[\frac{m}{2}\right] \pmod{2^{3+\operatorname{ord}_2 k}} & \text{otherwise.} \end{cases}$$

Proof It is easily proved by induction on s that for an odd integer j and $s \geq 1$

$$j^{2^s} \equiv \begin{cases} 1 \pmod{2^{s+3}} & \text{if } j \equiv \pm 1 \pmod 8, \\ 2^{s+2} + 1 \pmod{2^{s+3}} & \text{if } j \equiv \pm 3 \pmod 8. \end{cases}$$

Note that $k \geq 3 + \operatorname{ord}_2 k$. Indeed, for $\operatorname{ord}_2 k = 1$ and $\operatorname{ord}_2 k = 2$ it follows from the condition $k \geq 6$ and for $\operatorname{ord}_2 k \geq 3$ we have $k \geq 2^{\operatorname{ord}_2 k} \geq 3 + \operatorname{ord}_2 k$. Thus for an integer j we have

$$j^k \equiv \begin{cases} 0 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } j \text{ is even}, \\ 1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } j \equiv \pm 1 \pmod 8, \\ 2^{2+\operatorname{ord}_2 k} + 1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } j \equiv \pm 3 \pmod 8. \end{cases}$$

Assume that $m \equiv 1 \pmod 4$. Then

$$\#\{1 \leq n < m : n \equiv \pm 1 \pmod 8\} = \#\{1 \leq n < m : n \equiv \pm 3 \pmod 8\} = \frac{m-1}{4}.$$

Hence

$$\begin{aligned} S_k(m) &\equiv \frac{m-1}{4} + \frac{m-1}{4}\left(2^{2+\operatorname{ord}_2 k} + 1\right) \equiv \frac{m-1}{2}\left(2^{1+\operatorname{ord}_2 k} + 1\right) \\ &\equiv \begin{cases} \frac{m-1}{2} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 1 \pmod 8, \\ \frac{m-1}{2} + 2^{2+\operatorname{ord}_2 k} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 5 \pmod 8. \end{cases} \end{aligned}$$

Now assume that $m \equiv 3 \pmod 4$. Then

$$\#\{1 \le n \le m : n \equiv \pm 1 \pmod 8\} = \#\{1 \le n \le m : n \equiv \pm 3 \pmod 8\} = \frac{m+1}{4}.$$

This yields

$$\begin{aligned} S_k(m+1) &\equiv \frac{m+1}{4} + \frac{m+1}{4}\left(2^{2+\operatorname{ord}_2 k}+1\right) \equiv \frac{m+1}{2}\left(2^{1+\operatorname{ord}_2 k}+1\right) \\ &\equiv \begin{cases} \frac{m+1}{2} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 7 \pmod 8, \\ \frac{m+1}{2} + 2^{2+\operatorname{ord}_2 k} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 3 \pmod 8. \end{cases} \end{aligned}$$

Since

$$m^k \equiv \begin{cases} 1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 7 \pmod 8, \\ 2^{2+\operatorname{ord}_2 k}+1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 3 \pmod 8, \end{cases}$$

we deduce that

$$S_k(m) = S_k(m+1) - m^k \equiv \frac{m-1}{2} \pmod{2^{3+\operatorname{ord}_2 k}}.$$

Finally, if m is even, then

$$S_k(m) \equiv S_k(m+1) \equiv \begin{cases} \frac{m}{2} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \not\equiv 4 \pmod 8, \\ \frac{m}{2} + 2^{2+\operatorname{ord}_2 k} \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } m \equiv 4 \pmod 8. \end{cases}$$

This completes the proof.

Proof of Theorem 10.1 By Lemma 10.2 and Corollaries 3.8 and 8.2,

$$S_k(m) \equiv \frac{m-1}{2} \pmod{2^{3+\operatorname{ord}_2 k}}.$$

From Lemma 8.3 we see that

$$m \equiv \begin{cases} 7 \pmod 8 & \text{if } a \equiv 3 \pmod 4, \\ 3 \pmod 8 & \text{if } a \equiv 1 \pmod 4. \end{cases}$$

Therefore

$$aS_k(m) \equiv a \cdot \frac{m-1}{2} \equiv m^k \equiv \begin{cases} 1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } a \equiv 3 \pmod 4, \\ 2^{2+\operatorname{ord}_2 k}+1 \pmod{2^{3+\operatorname{ord}_2 k}} & \text{if } a \equiv 1 \pmod 4, \end{cases}$$

and so

$$a(m-1)-2 \equiv \begin{cases} 0 \pmod{2^{4+\mathrm{ord}_2\, k}} & \text{if } a \equiv 3 \pmod 4, \\ 2^{3+\mathrm{ord}_2\, k} \pmod{2^{4+\mathrm{ord}_2\, k}} & \text{if } a \equiv 1 \pmod 4, \end{cases}$$

as desired.

Theorem 10.3 *Let $a > 3$. If $aS_k(m) = m^k$ and m is a prime, then $a = q^{2s}$ for some irregular prime $q \equiv 3 \pmod{16}$ and positive integer s.*

Proof If a has at least two distinct prime divisors, then m cannot be a prime. Now assume that a is a power of a prime q. Then q is an irregular prime and $m = q$. Suppose that $a = q^{2s+1}$ for some $s \geq 0$. Then $(a+1)m^k/a(m+1) = (q^{2s+1}+1)S_k(q)/(q+1)$ is an integer, and (8.3) implies

$$\sum_{\substack{p|(q+1) \\ (p-1)|k}} \frac{1}{p} \equiv 0 \pmod 1.$$

Exactly as in the proof of Theorem 8.4, we conclude that this is impossible. Finally, assume that $a = q^{2s}$ for some $s \geq 1$. Then $a \equiv 1 \pmod 8$. Note that k has to be even. By Theorem 10.1 it follows that $a(q-1) \equiv 2 \pmod{16}$, which yields $\frac{q-1}{2} \equiv 1 \pmod 8$, that is, $q \equiv 3 \pmod{16}$.

`Remark` It is not known whether there are infinitely many irregular primes $q \equiv 3 \pmod{16}$. However, from a result of Metsänkylä [13] it follows that there are infinitely many irregular primes $q \equiv \pm 3, \pm 5 \pmod{16}$.

Acknowledgements This paper was begun during the stay of the first author in February–April 2014 at the Max Planck Institute for Mathematics. She likes to thank for the invitation and the pleasant research atmosphere. The second author was introduced to the subject around 1990 by the late Jerzy Urbanowicz. He will never forget his interest, help and kindness. Further he thanks Prof. T.N. Shorey for helpful discussions in the summer of 2014. We would like to heartily thank Bernd Kellner for helpful e-mail correspondence and patiently answering our Bernoulli number questions. A. Ciolan, P. Tegelaar and W. Zudilin kindly commented on an earlier version of this paper.

The cooperation of the authors has its origin in them having met, in 2012, at ELAZ in Schloss Schney (which was also attended by Prof. W. Schwarz). This contribution is our tribute to Prof. W. Schwarz, who was one of the initiators of the ELAZ conference series.

Appendix

Table 1 Pairs of irregular primes (p_1, p_2) with $p_1 < p_2$, $p_1 p_2 < 50000$, satisfying the conditions of Corollary 3.13

p_1	p_2
37	67, 103, 149, 157, 271, 307, 379, 401, 409, 421, 433, 463, 523, 541, 547, 557, 577, 593, 607, 613, 631, 673, 727, 757, 811, 877, 881, 1061, 1117, 1129, 1153, 1193, 1201, 1237, 1297, 1327
59	233, 523
67	103, 157, 271, 283, 409, 421, 433, 463, 541, 547, 613, 617, 619, 683, 691, 727
101	131, 149, 157, 271, 311, 401, 409, 421, 433, 461
103	157, 283, 307, 463
131	157, 271
149	233, 257, 293
157	233, 257, 271, 293, 307

Table 2 Helpful pairs $(t, q)_a$ with $q \leq 17$

q	t	$a \pmod q$
5	2	1, 2, 3
7	2	1, 3, 5
7	4	1, 3, 5
11	2	1, 2, 3, 5, 6, 7
11	4	2, 3, 6, 7, 9
11	6	1, 5, 6, 7
11	8	6, 7, 9
13	2	1, 2, 5, 6, 8, 10, 11
13	4	1, 2, 6, 8, 11
13	6	2, 3, 4, 5, 7, 8, 9, 10, 11
13	8	1, 2, 6, 8, 11
13	10	1, 2, 4, 6, 7, 8, 11
17	2	1, 2, 5, 7, 8, 10, 13, 14
17	4	1, 2, 3, 5, 8, 9, 11, 12, 15
17	6	1, 2, 4, 5, 6, 8
17	8	2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15
17	10	3, 7, 9, 11, 12, 14, 15
17	12	1, 2, 3, 5, 7, 8, 12, 14, 15
17	14	3, 4, 6, 7, 9, 11, 12, 14, 15

Table 3 Irregular pairs (r, p) along with the corresponding helpful pairs $(t_j, q_j)_{a \pmod{q_j}}$ satisfying the conditions of Proposition 4.5

a	Irregular pair (r, p)	ℓ_r	Helpful pairs $(t_j, q_j)_{a \pmod{q_j}}$
37	$(32, 37)$	1	$(8, 13)_{11}$
59	$(44, 59)$	6	$(2, 7)_3, (4, 7)_3, (6, 13)_7, (276, 349)_{59}$
67	$(58, 67)$	2	$(4, 13)_2, (10, 13)_2$
101	$(68, 101)$	6	$(2, 7)_3, (4, 7)_3, (28, 41)_{19}, (168, 601)_{101}$
103	$(24, 103)$	14	$(2, 5)_3, (16, 29)_{16}, (24, 43)_{17}, (92, 239)_{103}$, $(194, 239)_{103}, (228, 239)_{103}, (636, 1429)_{103}$, $(840, 1429)_{103}$
131	$(22, 131)$	4	$(2, 5)_1, (12, 41)_8, (152, 521)_{131}$
149	$(130, 149)$	15	$(2, 11)_6, (4, 11)_6, (6, 11)_6, (8, 11)_6, (2, 13)_6$, $(10, 13)_6, (30, 61)_{27}$
157	$(62, 157)$	1	$(2, 5)_2$
	$(110, 157)$	1	$(2, 5)_2$
233	$(84, 233)$	1	$(26, 59)_{56}$
257	$(164, 257)$	1	$(4, 17)_2$
263	$(100, 263)$	30	$(2, 5)_3, (2, 31)_{15}, (4, 31)_{15}, (8, 31)_{15}, (14, 31)_{15}$, $(16, 31)_{15}, (22, 31)_{15}, (28, 31)_{15}, (40, 61)_{19}$, $(624, 787)_{263}, (2196, 2621)_{263}, (2720, 3931)_{263}$
271	$(84, 271)$	1	$(4, 11)_7$
283	$(20, 283)$	1	$(2, 7)_3$
293	$(156, 293)$	30	$(2, 11)_7, (4, 11)_7, (6, 11)_7, (8, 11)_7, (20, 41)_6$, $(40, 61)_{49}, (740, 877)_{293}, (1032, 1753)_{293}$
307	$(88, 307)$	1	$(88, 103)_{101}$
311	$(292, 311)$	1	$(2, 11)_3$
347	$(280, 347)$	30	$(2, 5)_2, (2, 11)_6, (4, 11)_6, (6, 11)_6, (8, 11)_6$, $(10, 31)_6, (20, 61)_{42}, (972, 1039)_{347}$
353	$(186, 353)$	1	$(2, 5)_3$
	$(300, 353)$	9	$(2, 7)_3, (4, 7)_3, (12, 37)_{20}, (24, 37)_{20}, (36, 73)_{61}$
379	$(100, 379)$	1	$(4, 7)_1$
	$(174, 379)$	1	$(48, 127)_{99}$
389	$(200, 389)$	4	$(4, 17)_{15}, (8, 17)_{15}, (12, 17)_{15}, (976, 1553)_{389}$
401	$(382, 401)$	1	$(2, 5)_1$
409	$(126, 409)$	3	$(6, 19)_{10}, (12, 19)_{10}, (18, 37)_2$
421	$(240, 421)$	2	$(20, 41)_{11}, (240, 281)_{140}$
433	$(366, 433)$	1	$(2, 5)_3$
461	$(196, 461)$	1	$(12, 47)_{38}$
463	$(130, 463)$	1	$(4, 7)_1$
467	$(94, 467)$	3	$(2, 7)_5, (4, 7)_5, (1026, 1399)_{467}$
	$(194, 467)$	18	$(2, 5)_2, (2, 7)_5, (4, 7)_5, (12, 37)_{23}, (24, 37)_{23}$, $(3456, 8389)_{467}$

(continued)

Table 3 (continued)

a	Irregular pair (r, p)	ℓ_r	Helpful pairs $(t_j, q_j)_{a \pmod{q_j}}$
491	$(292, 491)$	1	$(2, 11)_7$
	$(336, 491)$	1	$(6, 11)_7$
	$(338, 491)$	1	$(8, 11)_7$
523	$(400, 523)$	1	$(4, 7)_5$
541	$(86, 541)$	1	$(2, 5)_1$
547	$(270, 547)$	1	$(36, 79)_{73}$
	$(486, 547)$	2	$(2, 5)_2, (96, 157)_{76}$
557	$(222, 557)$	1	$(2, 5)_2$
577	$(52, 577)$	1	$(4, 7)_3$
587	$(90, 587)$	6	$(2, 13)_2, (4, 13)_2, (6, 13)_2, (8, 13)_2, (10, 13)_2,$ $(90, 1759)_{587}$
	$(92, 587)$	6	$(2, 13)_2, (4, 13)_2, (6, 13)_2, (8, 13)_2, (10, 13)_2,$ $(678, 1759)_{587}$
593	$(22, 593)$	1	$(2, 5)_3$
607	$(592, 607)$	1	$(4, 7)_5$
613	$(522, 613)$	1	$(2, 5)_3$
617	$(20, 617)$	1	$(20, 29)_8$
	$(174, 617)$	1	$(2, 5)_2$
	$(338, 617)$	1	$(2, 5)_2$
619	$(428, 619)$	1	$(2, 7)_3$
631	$(80, 631)$	1	$(2, 7)_1$
	$(226, 631)$	1	$(4, 7)_1$
647	$(236, 647)$	6	$(2, 5)_2, (2, 7)_3, (4, 7)_3, (84, 229)_{189}$
	$(242, 647)$	3	$(2, 7)_3, (4, 7)_3, (72, 103)_{29}$
	$(554, 647)$	12	$(2, 5)_2, (2, 7)_3, (4, 7)_3, (180, 409)_{238},$ $(288, 457)_{190}$
653	$(48, 653)$	60	$(8, 17)_7, (12, 17)_7, (4, 31)_2, (14, 31)_2, (12, 41)_{38},$ $(20, 41)_{38}, (28, 41)_{38}, (24, 61)_{43}, (36, 61)_{43},$ $(196, 241)_{171}, (48, 2609)_{653}, (9176, 9781)_{653}$
659	$(224, 659)$	18	$(2, 7)_1, (4, 7)_1, (6, 13)_9, (12, 19)_{13}, (42, 127)_{24},$ $(882, 5923)_{659}$
673	$(408, 673)$	1	$(8, 17)_{10}$
	$(502, 673)$	1	$(2, 5)_3$
677	$(628, 677)$	3	$(4, 13)_1, (8, 13)_1, (30, 79)_{45}$
683	$(32, 683)$	12	$(2, 5)_3, (32, 67)_{13}, (76, 89)_{60}, (280, 373)_{310},$ $(2760, 4093)_{683}$
691	$(12, 691)$	1	$(12, 31)_9$
	$(200, 691)$	1	$(2, 7)_5$
727	$(378, 727)$	1	$(4, 23)_{14}$
751	$(290, 751)$	1	$(40, 251)_{249}$

(continued)

Table 3 (continued)

a	Irregular pair (r, p)	ℓ_r	Helpful pairs $(t_j, q_j)_{a \pmod{q_j}}$
757	(514, 757)	1	$(2, 5)_2$
761	(260, 761)	1	$(20, 41)_{23}$
773	(732, 773)	60	$(2, 7)_3, (4, 7)_3, (2, 11)_3, (4, 11)_3, (4, 17)_8,$ $(12, 17)_8, (16, 41)_{35}, (120, 241)_{50},$ $(1118, 1931)_{773}, (1504, 3089)_{773}$
797	(220, 797)	9	$(8, 37)_{20}, (20, 37)_{20}, (220, 2389)_{797},$ $(1812, 2389)_{797}, (2210, 3583)_{797}$
809	(330, 809)	5	$(2, 11)_6, (4, 11)_6, (6, 11)_6, (8, 11)_6, (10, 41)_{30}$
	(628, 809)	5	$(2, 11)_6, (4, 11)_6, (6, 11)_6, (8, 11)_6, (20, 41)_{30}$
811	(544, 811)	1	$(4, 19)_{13}$
821	(744, 821)	1	$(4, 11)_7$
827	(102, 827)	6	$(2, 13)_8, (4, 13)_8, (6, 13)_8, (8, 13)_8, (10, 13)_8,$ $(2580, 4957)_{827}$
839	(66, 839)	1680	$(2, 11)_3, (4, 11)_3, (6, 13)_7, (10, 13)_7, (8, 17)_6,$ $(2, 29)_{27}, (4, 29)_{27}, (8, 29)_{27}, (10, 29)_{27},$ $(12, 29)_{27}, (14, 29)_{27}, (16, 29)_{27}, (18, 29)_{27},$ $(20, 29)_{27}, (22, 29)_{27}, (10, 31)_2, (20, 31)_2,$ $(10, 41)_{19}, (16, 41)_{19}, (20, 41)_{19}, (26, 41)_{19},$ $(28, 41)_{19}, (30, 41)_{19}, (38, 41)_{19}, (28, 61)_{46},$ $(48, 61)_{46}, (56, 61)_{46}, (28, 71)_{58}, (56, 71)_{58},$ $(4, 97)_{63}, (52, 97)_{63}, (76, 97)_{63}, (26, 211)_{206},$ $(66, 211)_{206}, (6, 281)_{277}, (80, 281)_{277},$ $(138, 281)_{277}, (248, 281)_{277}, (258, 281)_{277},$ $(220, 673)_{166}, (17664, 20113)_{839}$
877	(868, 877)	1	$(4, 13)_6$
881	(162, 881)	1	$(2, 5)_1$
887	(418, 887)	3	$(2, 7)_5, (4, 7)_5, (2190, 2659)_{887}$
929	(520, 929)	1	$(8, 17)_{11}$
	(820, 929)	1	$(4, 17)_{11}$
953	(156, 953)	1	$(20, 137)_{131}$
971	(166, 971)	42	$(2, 7)_5, (4, 7)_5, (2, 29)_{14}, (16, 29)_{14}, (18, 43)_{25},$ $(24, 43)_{25}, (36, 43)_{25}, (26, 71)_{48}, (56, 71)_{48},$ $(6, 211)_{127}$
1061	(474, 1061)	1	$(2, 5)_1$
1091	(888, 1091)	8	$(2, 5)_1, (4, 17)_3, (8, 17)_3, (12, 17)_3, (8, 41)_{25}$
1117	(794, 1117)	1	$(2, 5)_2$
1129	(348, 1129)	5	$(2, 11)_7, (4, 11)_7, (6, 11)_7, (8, 11)_7, (20, 41)_{22}$
1151	(534, 1151)	1	$(4, 11)_7$
	(784, 1151)	1	$(4, 11)_7$
	(968, 1151)	1	$(8, 11)_7$

(continued)

Table 3 (continued)

a	Irregular pair (r, p)	ℓ_r	Helpful pairs $(t_j, q_j)_{a \pmod{q_j}}$
1153	$(802, 1153)$	1	$(2, 5)_3$
1193	$(262, 1193)$	1	$(2, 5)_3$
1201	$(676, 1201)$	1	$(4, 17)_{11}$
1217	$(784, 1217)$	3	$(4, 13)_8, (8, 13)_8, (48, 97)_{53}$
	$(866, 1217)$	1	$(2, 17)_{10}$
	$(1118, 1217)$	3	$(2, 13)_8, (6, 13)_8, (10, 13)_8$
1229	$(784, 1229)$	28	$(4, 17)_5, (8, 17)_5, (12, 17)_5, (16, 29)_{11}$, $(32, 113)_{99}, (784, 8597)_{1229}, (2012, 8597)_{1229}$, $(3240, 8597)_{1229}, (5696, 8597)_{1229}$, $(6924, 8597)_{1229}$
1237	$(874, 1237)$	1	$(2, 5)_2$
1279	$(518, 1279)$	1	$(2, 7)_5$
1283	$(510, 1283)$	10	$(2, 5)_3, (2, 11)_7, (4, 11)_7, (6, 11)_7, (8, 11)_7$, $(6920, 12821)_{1283}$
1291	$(206, 1291)$	2	$(2, 5)_1, (56, 61)_{10}$
	$(824, 1291)$	1	$(14, 31)_{20}$
1297	$(202, 1297)$	1	$(2, 5)_2$
	$(220, 1297)$	1	$(12, 17)_5$
1301	$(176, 1301)$	1	$(20, 53)_{29}$
1307	$(382, 1307)$	3	$(2, 7)_5, (4, 7)_5, (2994, 3919)_{1307}$
	$(852, 1307)$	3	$(2, 7)_5, (4, 7)_5, (852, 3919)_{1307}$
1319	$(304, 1319)$	360	$(2, 7)_3, (4, 7)_3, (8, 17)_{10}, (6, 31)_{17}, (12, 31)_{17}$, $(18, 31)_{17}, (24, 31)_{17}, (6, 37)_{24}, (12, 37)_{24}$, $(18, 37)_{24}, (30, 73)_5, (36, 73)_5, (66, 73)_5$, $(2940, 11863)_{1319}, (42480, 52721)_{1319}$
1327	$(466, 1327)$	2	$(2, 5)_2, (4, 13)_1$
1367	$(234, 1367)$	6	$(2, 5)_2, (4, 13)_2, (8, 13)_2, (234, 4099)_{1367}$
1369	$(32, 37)$	10	$(2, 11)_5, (6, 11)_5, (14, 31)_5, (8, 41)_{16}, (20, 61)_{27}$
1381	$(266, 1381)$	1	$(2, 5)_1$
1409	$(358, 1409)$	1	$(6, 23)_6$
1429	$(996, 1429)$	1	$(44, 239)_{234}$
1439	$(574, 1439)$	630	$(4, 11)_9, (8, 11)_9, (2, 19)_{14}, (4, 19)_{14}, (8, 19)_{14}$, $(10, 19)_{14}, (12, 19)_{14}, (2, 31)_{13}, (6, 31)_{13}$, $(12, 31)_{13}, (22, 31)_{13}, (26, 31)_{13}, (24, 37)_{33}$, $(6, 43)_{20}, (24, 43)_{20}, (10, 61)_{36}, (30, 61)_{36}$, $(40, 61)_{36}, (30, 71)_{19}, (40, 71)_{19}, (36, 127)_{42}$, $(16, 181)_{172}, (50, 181)_{172}, (140, 181)_{172}$, $(60, 211)_{173}, (574, 8629)_{1439}, (50904, 60397)_{1439}$
1483	$(224, 1483)$	2	$(2, 13)_1, (8, 13)_1$
1499	$(94, 1499)$	24	$(2, 7)_1, (4, 7)_1, (6, 13)_4, (4, 17)_3, (8, 17)_3$, $(10, 17)_3, (12, 17)_3, (14, 17)_3, (736, 857)_{642}$

References

1. T. Arakawa, T. Ibukiyama, M. Kaneko, *Bernoulli Numbers and Zeta Functions*. Springer Monographs in Mathematics (Springer, Tokyo, 2014)
2. E. Bach, D. Klyve, J. Sorenson, Computing prime harmonic sums. Math. Comput. **78**, 2283–2305 (2009)
3. J.M. Borwein, A. van der Poorten, J. Shallit, W. Zudilin, *Neverending Fractions: An Introduction to Continued Fractions*. Australian Mathematical Society Lecture Series, vol. 23 (Cambridge University Press, Cambridge, 2014)
4. W. Butske, L.M. Jaje, D.R. Mayernik, On the equation $\sum_{p|N}(1/p)+(1/N) = 1$, pseudoperfect numbers, and perfectly weighted graphs. Math. Comput. **69**, 407–420 (2000)
5. L. Carlitz, Note on irregular primes. Proc. Am. Math. Soc. **5**, 329–331 (1954)
6. Y. Gallot, P. Moree, W. Zudilin, The Erdős-Moser equation $1^k + 2^k + \cdots + (m-1)^k = m^k$ revisited using continued fractions. Math. Comput. **80**, 1221–1237 (2011)
7. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer, New York, 1990)
8. B.C. Kellner, Über irreguläre Paare höherer Ordnungen, Diplomarbeit, Mathematisches Institut der Georg–August–Universität zu Göttingen, Germany (2002). Also available at http://www.bernoulli.org/~bk/irrpairord.pdf
9. B.C. Kellner, On irregular prime power divisors of the Bernoulli numbers. Math. Comput. **76**, 405–441 (2007)
10. B.C. Kellner, On stronger conjectures that imply the Erdős-Moser conjecture. J. Number Theory **131**, 1054–1061 (2011)
11. E.E. Kummer, Allgemeiner Beweis des Fermatschen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $(\lambda-3)/2$ Bernoullischen Zahlen als Factoren nicht vorkommen. J. Reine Angew. Math. **40**, 131–138 (1850)
12. F. Luca, A. Pizarro-Madariaga, C. Pomerance, On the counting function of irregular primes. Indag. Math. **26**, 147–161 (2015)
13. T. Metsänkylä, Distribution of irregular prime numbers. J. Reine Angew. Math. **282**, 126–130 (1976)
14. P. Moree, On a theorem of Carlitz-von Staudt. C. R. Math. Rep. Acad. Sci. Canada **16**, 166–170 (1994)
15. P. Moree, Diophantine equations of Erdős-Moser type. Bull. Aust. Math. Soc. **53**, 281–292 (1996)
16. P. Moree, A top hat for Moser's four mathemagical rabbits. Am. Math. Mon. **118**, 364–370 (2011)
17. P. Moree, Moser's mathemagical work on the equation $1^k + 2^k + \cdots + (m-1)^k = m^k$. Rocky Mt. J. Math. **43**, 1707–1737 (2013)
18. P. Moree, Counting numbers in multiplicative sets: Landau versus Ramanujan. Šiauliai Math. Semin. **8**(16), 161–179 (2013)
19. P. Moree, H. te Riele, J. Urbanowicz, Divisibility properties of integers x, k satisfying $1^k + \cdots + (x-1)^k = x^k$. Math. Comput. **63**, 799–815 (1994)
20. L. Moser, On the diophantine equation $1^n + 2^n + 3^n + \cdots + (m-1)^n = m^n$. Scr. Math. **19**, 84–88 (1953)
21. P. Ribenboim, *Catalan's Conjecture. Are 8 and 9 the only Consecutive Powers?* (Academic, Boston, 1994)
22. W. Schwarz, J. Spilker, *Arithmetical Functions*. London Mathematical Society Lecture Note Series, vol. 184 (Cambridge University Press, Cambridge, 1994)
23. C.L. Siegel, Zu zwei Bemerkungen Kummers. Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **6**, 51–57 (1964)
24. P. Tegelaar, Handwritten comments on an earlier version of this paper, March 6, 2015

A Note on the Negative Pell Equation

Valentin Blomer

To the memory of Wolfgang Schwarz

Abstract Nagell conjectured in the 1930s that the set of discriminants for which the negative Pell equation has an integral solution has an explicitly given positive proportion within the set of discriminants having no prime factor congruent to 3 modulo 4. In a series of papers, Fouvry and Klüners succeeded in showing that the order of magnitude of such discriminants up to x is indeed $x(\log x)^{-1/2}$. Here we present a short independent argument that the order of magnitude is at least $x(\log x)^{-0.62}$.

Keywords Fundamental unit • Negative norm • Number of discriminants • Pell equation

2010 Mathematics subject classification: Primary 11N45; Secondary 11D09

1 Introduction

There are many open questions in connection with the solvability and the size of possible solutions of Pell-type equations

$$x^2 - dy^2 = C, \quad x, y \in \mathbb{Z}, \tag{1.1}$$

for given squarefree $d > 0$. Let us write $K := \mathbb{Q}(\sqrt{d})$ and

$$D := \operatorname{disc} K/\mathbb{Q} = f^2 d, \quad f \in \{1, 2\}.$$

V. Blomer (✉)
Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany
e-mail: vblomer@math.uni-goettingen.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_2

While (1.1) has always integral solutions for $C = 1$, only some d admit integral solutions to

$$x^2 - dy^2 = -1. \tag{1.2}$$

This is tantamount to asking for which real quadratic discriminants D the fundamental unit ϵ_D has negative norm, $N\epsilon_D = -1$. Let $\mathfrak{D}$ be the set of such discriminants. It is well known that $D \in \mathfrak{D}$ if and only if the period length of the continued fraction of $\sqrt{d}$ is odd (which, however, might be as long as about $\sqrt{d}$). In more algebraic terms, (1.2) is solvable in $x, y \in \mathbb{Z}$ if and only if the class group of K coincides with the narrow class group, in other words if the narrow Hilbert class field of K is real. It is, however, a hard problem to find necessary and sufficient criteria for $\mathfrak{D}$ that are both efficient from an algorithmic point of view and simple enough for theoretical purposes, e.g. counting the number of $D \in \mathfrak{D}$ up to x.

Let $\mathcal{S}$ be the set of integers having no prime divisor $p \equiv 3 \pmod 4$. By the Hasse principle we see that (1.2) admits *rational* solutions if and only if $d \in \mathcal{S}$, in particular

$$\#\{D \le x \mid D \in \mathfrak{D}\} \le \#\{\text{discriminants } D \le x \mid D \in \mathcal{S}\} \ll \frac{x}{\sqrt{\log x}}.$$

On the other hand, by an observation of Redei the negative Pell equation does have integral solutions if $d \in \mathcal{S}$ and in addition the two-part $\mathcal{C}[2]$ of the class group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(D)-1}$, that is, the class group $\mathcal{C}$ of K has no element of order 4. For, in the latter case, the narrow 2-Hilbert class field coincides with the genus field and is in particular real. In other words, if $\mathcal{D}$ denotes the set of discriminants of real quadratic fields in $\mathcal{S}$ with no element of order 4 in the class group, then $\mathcal{D} \subseteq \mathfrak{D}$.

On probabilistic grounds, one may expect

$$\#\{D \le x \mid D \in \mathfrak{D}\} \asymp \frac{x}{\sqrt{\log x}}; \tag{1.3}$$

more precisely, there is theoretical and (some) empirical evidence [8] that

$$\frac{\#\{D \le x \mid D \in \mathfrak{D}\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}\}} \sim 1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{2^{2j-1}}\right) \approx 0.581, \quad x \to \infty. \tag{1.4}$$

Nagell [6] conjectured more than 80 years ago that the limit (1.4) exists in the open interval $(0, 1)$, but no proof has been found so far. The beauty in this conjecture lies in the mix of analytic and algebraic number theory that is already apparent in the formulation of the problem.

A first step was made by Cremona and Odoni who proved ([1], see also [8])

$$\frac{\#\{D \le x \mid D \in \mathcal{D}, \omega(D) = n\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}, \omega(D) = n\}} \sim \prod_{j=1}^{n/2} \left(1 - \frac{1}{2^{2j-1}}\right), \quad x \to \infty \tag{1.5}$$

for each fixed $n \in \mathbb{N}$, so that in particular

$$\#\{D \le x \mid D \in \mathfrak{D}\} \gg_n \frac{x(\log\log x)^n}{\log x}. \tag{1.6}$$

In an impressive series of long and difficult papers, Fouvry and Klüners [3–5] made great progress and essentially solved the problem (along with several related questions) by showing that the left-hand side of (1.4) is asymptotically bounded between two constants:

$$0.524 \le \frac{5}{4} \prod_{j=1}^{\infty} \left(1 - \frac{1}{2^{2j-1}}\right) + o(1) \le \frac{\#\{D \le x \mid D \in \mathfrak{D}\}}{\#\{\text{discriminants } D \le x \mid D \in \mathcal{S}\}} \le \frac{2}{3} + o(1).$$

Our goal in this note is much more modest. Here we show that a short argument suffices to bring us half-way between (1.6) and the correct order of magnitude $x(\log x)^{-1/2}$.

Theorem 1.1 *Let $\alpha_0 = 0.616\ldots$ be the minimum of the function*

$$f(\alpha) := 1 - \alpha\left(1 + \log\frac{1 - \alpha\log 2}{2\alpha}\right).$$

Then

$$\#\{D \le x \mid D \in \mathfrak{D}\} \gg_\varepsilon \frac{x}{(\log x)^{\alpha_0+\varepsilon}}$$

for any $\varepsilon > 0$.

The general approach is similar as in [1], but we modify the argument as follows: (a) we only aim at getting lower bounds for the quantity on the left-hand side of (1.5), (b) we use the large sieve to estimate primes in arithmetic progressions on average and (c) we exclude exceptional (Siegel) discriminants at an early stage of the argument. The idea of the method dates back several years, and Theorem 1.1 is already mentioned in [4].

2 Proof of the Theorem

We start with the Siegel–Walfisz Theorem (e.g. [2, Sect. 20]). Let $(a, q) = 1$. There is a constant $C > 0$ such that

$$\pi(x; q, a) := \sum_{\substack{n \le x \\ n \equiv a \,(\mathrm{mod}\, q)}} 1 = \frac{1}{\phi(q)} \int_2^x \frac{dt}{\log t} + O\left(xe^{-C\sqrt{\log x}}\right) \tag{2.1}$$

for all $q \le e^{\sqrt{\log x}}$, except possibly for a thin sequence $q_1 < q_2 < \dots$ satisfying $q_{j+1} > q_j^2$. In particular, there is a set of rational primes $\mathcal{P} := \{\pi_1, \pi_2, \dots\}$ with $\pi_n > 2^{2^{n-1}}$ such that (2.1) holds for all $q \le e^{\sqrt{\log x}}$ not divisible by any of the π_j.

Our aim is to find a lower bound for the number of $D \in \mathcal{D}$ which implies automatically a lower bound for the number of $D \in \mathfrak{D}$. To this end we utilize a criterion of Redei–Reichardt to characterize the 4-rank of the class group. Let

$$\mathcal{D}^* := \{D \in \mathbb{N} \mid \mu^2(D) = 1,\ p \mid D \Rightarrow (p \equiv 1 \,(\mathrm{mod}\, 4), p \notin \mathcal{P})\},$$
$$\mathcal{D}_n^* := \{D \in \mathcal{D}^* \mid \omega(D) = n\},$$

and let

$$\mathfrak{U}_n := \{(u_{ij})_{1 \le i,j \le n} \mid u_{ij} = 0 \text{ for } j \ge i, u_{ij} \in \{\pm 1\} \text{ for } 1 \le i < j \le n\} = \left\{ \begin{pmatrix} 0 & & \pm 1 \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \right\}.$$

For any $D = \prod_{i=1}^n p_i \in \mathcal{D}_n^*$ let $(\varepsilon_{ij}) =: \mathcal{U}(D) \in \mathfrak{U}_n$ be given by $\varepsilon_{ij} := \left(\frac{p_i}{p_j}\right)$ for $i < j$. Then the 4-rank of the class group of $\mathbb{Q}(\sqrt{D})$ is determined by $\mathcal{U}(D)$ in the following way. Let $\tilde{\mathcal{U}}(D) := (\eta_{ij}) \in \mathbb{F}_2^{n \times n}$ be defined by $(-1)^{\eta_{ij}} = \varepsilon_{ij}$ for $i < j$, $\eta_{ij} = \eta_{ji}$ and $\eta_{ii} = \sum_{j \ne i} \eta_{ij}$. Then by a criterion of Redei–Reichardt [7] (see also [8]),

$$4\text{-rank of the class group of } \mathbb{Q}(\sqrt{D}) = n - 1 - \mathrm{rk}_{\mathbb{F}_2} \tilde{\mathcal{U}}(D). \tag{2.2}$$

We shall need the following lemma [1, Proposition 2.5]:

Lemma 2.1 *Out of the* $2^{\binom{n}{2}}$ *matrices* $\mathcal{U} \in \mathfrak{U}_n$ *exactly*

$$2^{\binom{n}{2}} \prod_{j=1}^{n/2} \left(1 - \frac{1}{2^{2j-1}}\right) \gg 2^{\binom{n}{2}}$$

matrices give rise to a matrix $\tilde{\mathcal{U}}$ *having rank* $n - 1$ *over* $\mathbb{F}_2$.

For any $\mathcal{V} \in \mathfrak{U}_n$ let

$$\mathcal{D}_n^*(x, \mathcal{V}) := \#\{D \in \mathcal{D}_n^* \mid D \le x, \mathcal{U}(D) = \mathcal{V}\}.$$

The idea is to estimate this quantity from below, sum over all admissible $\mathcal{V}$ and then optimize the value of n. To this end, let us fix a small $\varepsilon > 0$, let $C(\varepsilon)$ be a sufficiently large constant depending only on ε, and let

$$\gamma_n := C(\varepsilon)^{(2+4\varepsilon)^{n-1}}.$$

In the following, all implied constant may depend on ε, but not on n. We shall show by induction:

$$\mathcal{D}_n^*(x, \mathcal{V}) \gg_\varepsilon \Xi_n 2^{-\binom{n}{2}} \frac{x}{\log x} \frac{(\log\log x - \log\log \gamma_n)^{n-1}}{2^n (n-1)!} \tag{2.3}$$

for any $\mathcal{V} \in \mathfrak{U}_n$ and $x > \gamma_n$ where

$$\Xi_n := \prod_{j=1}^{n} \left(1 - \frac{c(\varepsilon)\exp(j^2)}{\exp(c_1\sqrt{\log \gamma_j})}\right) \gg 1$$

for a suitable constant $c(\varepsilon) > 0$. Here we choose $C(\varepsilon)$ large enough (in terms of $c(\varepsilon)$ and c_1) so that each factor is positive. We will also choose $n \le \log\log x$, so that $\gamma_n \le \exp(\log C(\varepsilon) \cdot (\log x)^{0.7})$ for ε sufficiently small and the condition $\gamma_n < x$ is not void.

From Lemma 2.1, (2.2), (2.3) and the definition of $\mathcal{D}$, we find

$$\#\{D \in \mathcal{D} \mid D \le x\} \gg \frac{x}{\log x} \frac{(\log\log x - (n-1)\log(2+4\varepsilon) - \log\log C(\varepsilon))^{n-1}}{2^n (n-1)!}$$

for $n \le \log\log x$ (and sufficiently large x). Choosing $n = [\alpha \log\log x]$ for some real $0 < \alpha < 1$, this is by Stirling's formula

$$\gg \frac{x}{\log x} \left(\frac{1 - \alpha\log 2}{2} \frac{e}{\alpha}\right)^{(\alpha + o(1))\log\log x} = x(\log x)^{f(\alpha)+o(1)},$$

with $f(\alpha)$ as in Theorem 1.1, and the proof follows.

The rest of the paper is devoted to the proof of (2.3). This is certainly true for $n = 1$ by the prime number theorem (or Chebyshev-type estimates) for the progression 1 (mod 4). Suppose now (2.3) holds for some $n \in \mathbb{N}$, and let $\mathcal{V} = (\varepsilon_{ij})_{1 \le i,j \le n+1} \in \mathfrak{U}_{n+1}$ be given. Let $\mathcal{U} := (\varepsilon_{ij})_{1 \le i,j \le n} \in \mathfrak{U}_n$ be obtained by deleting the last row and column from $\mathcal{V}$. Let us consider some $t = \prod_{i=1}^{n} p_i \in \mathcal{D}^*(x, \mathcal{U})$. We denote by $\mathcal{A}_t$ the set of

residue classes $a \pmod{4t}$ satisfying

$$a \equiv 1 \pmod 4 \text{ and } \left(\frac{p_i}{a}\right) = \varepsilon_{i,n+1}, 1 \le i \le n.$$

By the Chinese remainder theorem we have

$$\#\mathcal{A}_t = \frac{\phi(4t)}{2^{n+1}}.$$

If p satisfies the three conditions $p \equiv a \pmod{4t}$ for some $a \in \mathcal{A}_t$, $p_n < p < x/t$, and $p \notin \mathcal{P}$, then $pt \in \mathcal{D}^*_{n+1}(x, \mathcal{V})$. Let us assume $x > \gamma_{n+1}$, and write

$$y := x^{(1-\varepsilon)/2}.$$

Without loss of generality we also assume that $x = [x] + \frac{1}{2}$ is a half-integer. Then we have

$$\begin{aligned}
\mathcal{D}^*_{n+1}(x, \mathcal{V}) &\ge \sum_{t=\prod p_i \in \mathcal{D}^*_n(y,\mathcal{U})} \sum_{a \in \mathcal{A}_t} \#\left\{p_n < p \le \frac{x}{t} \mid p \equiv a \pmod{4t}, p \notin \mathcal{P}\right\} \\
&= \sum_{t \in \mathcal{D}^*_n(y,\mathcal{U})} \sum_{a \in \mathcal{A}_t} \pi\left(\frac{x}{t}; 4t, a\right) + O\left(\sum_{t \le y}{}^* (\pi(t) + \#\{\pi \le x \mid \pi \in \mathcal{P}\})\right) \\
&= \frac{1}{2^{n+1}} \sum_{t \in \mathcal{D}^*_n(y,\mathcal{U})} \pi\left(\frac{x}{t}\right) + O\left(\sum_{t \le y}{}^* \sum_{a \in \mathcal{A}_t} \left|\pi\left(\frac{x}{t}; 4t, a\right) - \frac{\pi(x/t)}{\phi(4t)}\right|\right) \\
&\quad + O(x^{1-\varepsilon}),
\end{aligned} \tag{2.4}$$

where $\sum^*$ indicates that the summation is taken over t coprime to all $\pi \in \mathcal{P}$. By the prime number theorem and partial summation, the main term is

$$\begin{aligned}
&\ge \frac{1}{2^{n+1}} \sum_{t \in \mathcal{D}^*_n(y,\mathcal{U})} \int_2^{x/t} \frac{dt}{\log t} + O\left(\sum_{t \le y} \frac{x/t}{\exp(c_2\sqrt{\log(x/t)})}\right) \\
&\ge \frac{x}{2^{n+1}} \int_{\gamma_n}^{y} \frac{\mathcal{D}^*_n(u, \mathcal{V})}{u^2 \log(x/u)} du + O\left(\frac{x}{\exp(c_3\sqrt{\log x})}\right);
\end{aligned} \tag{2.5}$$

note that $y \le x^{1/2}$, so that $\log \frac{x}{t} \gg \log x$. By the induction hypothesis (2.3) the main term here is

$$\begin{aligned} &\ge \Xi_n 2^{-\binom{n}{2}} \frac{x}{2^{n+1}\log x} \int_{\gamma_n}^{y} \frac{(\log\log u - \log\log\gamma_n)^{n-1}}{2^n (n-1)! u \log u} du \\ &= \Xi_n 2^{-\binom{n}{2}} \frac{x}{2^{n+1}\log x} \frac{(\log\log y - \log\log\gamma_n)^n}{2^n n!} \\ &= \Xi_n 2^{-\binom{n+1}{2}} \frac{x}{\log x} \frac{(\log\log x - \log\frac{2}{1-\varepsilon} - \log\log\gamma_n)^n}{2^{n+1} n!}. \end{aligned} \tag{2.6}$$

It remains to estimate the first error term on the right-hand side of (2.4). This is a standard application of the large sieve. We split the t-sum in $O(\log x)$ dyadic segments. A typical of these terms is at most

$$\sideset{}{^*}\sum_{z\le t\le 2z} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, 4t)} \Bigg| \sum_{\substack{p\le x/t \\ p\equiv a \,(\mathrm{mod}\, 4t)}} 1 - \frac{1}{\phi(4t)} \sum_{p\le x/t} 1 \Bigg| \tag{2.7}$$

for $z \le y$. It is convenient to make the summation range independent of t by replacing the condition $p \le x/t$ with $p \le x/z$. This can be easily done by integral transforms. We use the formula (see, e.g., [2, p. 165])

$$\int_{-T}^{T} e^{i\xi\alpha} \frac{\sin(\xi\beta)}{\pi\xi} d\xi = \begin{cases} 1 + O((T(\beta - |\alpha|))^{-1}), & |\alpha| < \beta, \\ O((T(|\alpha| - \beta))^{-1}), & |\alpha| > \beta \end{cases}$$

for $T, \beta > 0$ with $\beta = \log X$, $\alpha = \log m$ getting

$$\sum_{m\le X} a_m = \int_{-T}^{T} \sum_{m\le Y} a_m m^{i\xi} \frac{\sin(\xi \log X)}{\pi\xi} d\xi + O\left(\frac{1}{T} \sum_{m\le Y} |a_m| \left| \log \frac{m}{X} \right|^{-1} \right)$$

for real numbers $Y \ge X$ and any sequence (a_m). In particular, (2.7) is at most

$$\begin{aligned} &\int_{-T}^{T} \sideset{}{^*}\sum_{z\le t\le 2z} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, 4t)} \Bigg| \sum_{\substack{p\le x/z \\ p\equiv a \,(\mathrm{mod}\, 4t)}} p^{i\xi} - \frac{1}{\phi(4t)} \sum_{p\le x/z} p^{i\xi} \Bigg| \min\left(\frac{1}{|\xi|}, \log x \right) d\xi \\ &+ O\left(\frac{1}{T} \sideset{}{^*}\sum_{z\le t\le 2z} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, 4t)} \left(\sum_{\substack{p\le x/z \\ p\equiv a \,(\mathrm{mod}\, 4t)}} \left| \log \frac{pt}{x} \right|^{-1} + \frac{1}{\phi(4t)} \sum_{p\le x/z} \left| \log \frac{pt}{x} \right|^{-1} \right) \right) \end{aligned} \tag{2.8}$$

for some $0 < T < x$ to be chosen later. Gluing together t and p, the error term in (2.8) is at most

$$\ll \frac{1}{T} \sum_{q \le 2x} d(q) \left| \log \frac{q}{x} \right|^{-1} \ll \frac{x(\log x)^2}{T}; \tag{2.9}$$

here we need our assumption that x is not too close to an integer. The main term in (2.8) is by Cauchy's inequality

$$\ll \int_{-T}^{T} \left(\sum_{z \le t \le 2z}^{*} \sum_{a \,(\mathrm{mod}\, 4t)}^{*} \left| \frac{1}{\phi(4t)} \sum_{\chi \ne \chi_0} \bar{\chi}(a) \sum_{p \le x/z} \chi(p) p^{i\xi} \right|^2 \right)^{1/2} z \min\left(\frac{1}{|\xi|}, \log x \right) d\xi.$$

We open the square and express each character modulo $4t$ in terms of its underlying primitive character modulo $t' = 4t/\ell$. Using $\phi(\ell t') \ge \phi(\ell)\phi(t')$ we get

$$\int_{-T}^{T} \left(\sum_{\ell \le x} \frac{1}{\phi(\ell)} \sum_{\frac{4z}{\ell} \le t' \le \frac{8z}{\ell}}^{*} \frac{1}{\phi(t')} \sum_{\chi \,(\mathrm{mod}\, t')}^{*} \left| \sum_{\substack{p \le x/z \\ (p,\ell)=1}} \chi(p) p^{i\xi} \right|^2 \right)^{1/2} z \min\left(\frac{1}{|\xi|}, \log x \right) d\xi. \tag{2.10}$$

We recall that the asterisk at the t'-sum denotes non-exceptional discriminants and the asterisk at the χ-sum denotes primitivity. We split the t'-sum into two parts, $t' \ge P$ and $t' < P$ for some $P \le \exp(\sqrt{\log x})$ to be chosen later. By the large sieve inequality (e.g. [2, p. 160]), the t'-sum restricted to $t' \ge P$ can be bounded by

$$\ll \left(\frac{x}{zP} + \frac{z}{\ell} \right) \pi\left(\frac{x}{z} \right);$$

summing over ℓ and integrating over ξ we get

$$\frac{x(\log x)^{3/2}}{\sqrt{P}} + x^{1-\frac{\varepsilon}{2}} \log x \tag{2.11}$$

since $z \le y = x^{(1-\varepsilon)/2}$. Let us now deal with the terms $t' < P$. In this case, the innermost p-sum in (2.10) equals

$$\sum_{b \,(\mathrm{mod}\, t')} \chi(b) \sum_{\substack{p \le x/z \\ p \equiv b \,(\mathrm{mod}\, t') \\ (p,\ell)=1}} p^{i\xi}.$$

By partial summation, and (2.1) where we use the fact that we have excluded exceptional characters, this double sum is

$$\ll t' \frac{x}{z} \exp\left(-C'\sqrt{\log \frac{x}{z}}\right)(1+|\xi|)$$

for some absolute constant $0 < C' < 1$ (without loss of generality). Therefore the terms $t' < P$ contribute at most

$$P^{3/2}x(T+\log x)\exp\left(-\frac{C'}{2}\sqrt{\log \frac{x}{z}}\right) \ll P^{3/2}x(T+\log x)\exp\left(-\frac{C'}{4}\sqrt{\log x}\right) \tag{2.12}$$

to (2.10) where we used again $z \le x^{1/2}$. Now we choose

$$T := \exp\left(\frac{C'}{20}\sqrt{\log x}\right), \quad P := \exp\left(\frac{C'}{10}\sqrt{\log x}\right).$$

Collecting the error terms (2.9), (2.11) and (2.12), we see that (2.7) is

$$\ll x(\log x)^2 \exp\left(-\frac{C'}{20}\sqrt{\log x}\right),$$

and thus the total error in (2.4) and (2.5) is at most

$$O\left(x\exp\left(-\min\left(\frac{C'}{30}, c_3\right)\sqrt{\log x}\right)\right).$$

For $x \ge \gamma_{n+1}$, the main term (2.6) is

$$\gg 2^{-\binom{n+1}{2}} \frac{x}{\log x} \frac{(\log(1+\varepsilon-2\varepsilon^2))^n}{2^{n+1}n!} \gg_\varepsilon \frac{x}{\log x} 2^{-(n+1)^2}.$$

Thus we can bound (2.4) from below by

$$\Xi_n 2^{-\binom{n+1}{2}} \frac{x}{\log x} \frac{(\log\log x - \log\log \gamma_{n+1})^n}{2^{n+1}n!}\left(1 - O_\varepsilon\left(\frac{\exp((n+1)^2)}{\exp\left(c_1\sqrt{\log \gamma_{n+1}}\right)}\right)\right)$$

for $x \ge \gamma_{n+1}$ and some $c_1 > 0$. This is exactly (2.3) for $n+1$.

References

1. J.E. Cremona, R.W.K. Odoni, Some density results for negative Pell equations; an application of graph theory. J. Lond. Math. Soc. **39**, 16–28 (1989)
2. H. Davenport, *Multiplicative Number Theory*, 2nd edn. (Springer, New York, 1980)
3. É. Fouvry, J. Klüners, On the 4-rank of class groups of quadratic number fields. Invent. Math. **167**, 455–513 (2007)
4. É. Fouvry, J. Klüners, On the negative Pell equation. Ann. Math. **172**, 2035–2104 (2010)
5. É. Fouvry, J. Klüners, The parity of the period of the continued fraction of $\sqrt{d}$. Proc. Lond. Math. Soc. **101**, 337–391 (2010)
6. T. Nagell, Über die Lösbarkeit der Gleichung $x^2 - Dy^2 = -1$, Ark. Mat. 23B, Nr. 6, 5 pp. (1933)
7. L. Redei, E. Reichardt, Die Anzahl der durch 4 teilbaren Invarianaten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J. Reine Angew. Math. **170**, 69–74 (1934)
8. P. Stevenhagen, The number of real quadratic fields having units of negative norm. Exp. Math. **2**, 121–136 (1993)

Localisation Conditionnelle de Diviseurs

Régis de la Bretèche and Gérald Tenenbaum

À la mémoire de Wolfgang Schwarz,
pour la délicatesse et la distinction

Abstract In support of a still little known, general principle according to which the structure of the set of prime factors of an integer is statistically governed by its actual cardinal, we show that, given any $\varepsilon > 0$, the conditional probability that an integer with exactly k prime factors has a divisor in a dyadic interval $]y, 2y]$ approaches 0 as $y \to \infty$ if $2^{(1+\varepsilon)k} < \log y$ while it remains larger than a strictly positive constant when $2^{(1-\varepsilon)k} > \log y$.

Keywords Distribution of divisors • Integers with k prime factors

2010 Mathematics subject classification: Primary 11N25

Résumé À l'appui d'un principe général peu connu selon lequel la structure de la suite des facteurs premiers d'un entier est statistiquement gouvernée par son cardinal global, nous montrons que, pour tout $\varepsilon > 0$, la probabilité conditionnelle pour qu'un entier ayant k facteurs premiers possède un diviseur dans un intervalle dyadique $]y, 2y]$ tend vers 0 lorsque $y \to \infty$ si $2^{(1+\varepsilon)k} < \log y$ mais qu'elle demeure plus grande qu'une constante strictement positive si $2^{(1-\varepsilon)k} > \log y$.

Mots-clefs Répartition des diviseurs • entiers ayant k facteurs premiers.

2010 Mathematics subject classification: Principale 11N25

R. de la Bretèche
Institut de Mathématiques de Jussieu-PRG, UMR 7586, Université Paris Diderot-Paris 7, Sorbonne Paris Cité, Case 7012, F-75013 Paris, France

UMR 7586, Institut de Mathématiques de Jussieu-PRG, Case 7012, F-75013 Paris, France
e-mail: regis.de-la-breteche@imj-prg.fr

G. Tenenbaum (✉)
Institut Élie Cartan, Université de Lorraine, BP 70239, 54506 Vandœuvre-lès-Nancy Cedex, France
e-mail: gerald.tenenbaum@univ-lorraine.fr

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_3

1 Introduction

La localisation de diviseurs dans des intervalles dyadiques pose un délicat problème de crible: aucune relation de divisibilité ne lie les entiers d'un intervalle $]y, 2y]$ ($y \geqslant 1$), mais les ensembles de multiples de deux éléments quelconques ne sont généralement pas indépendants.

Considérons la densité ε_y de l'ensemble $\mathscr{H}_y$ des entiers naturels ayant au moins un diviseur d tel que $y < d \leqslant 2y$. Besicovitch [3] a établi en 1934 que

$$\liminf_{y\to\infty} \varepsilon_y = 0$$

et en a déduit une remarquable réfutation de la conjecture en vigueur à l'époque selon laquelle tout ensemble de multiples admettrait une densité naturelle.

Erdős [5] a montré en 1936 que $\varepsilon_y \to 0$. Cependant, la détermination du véritable ordre de grandeur de ε_y a longtemps constitué un véritable défi pour les spécialistes. Précisant une estimation du second auteur [10], Ford [7] a montré en 2008 que l'on a

$$\varepsilon_y \asymp \frac{1}{(\log y)^{\delta}(\log_2 y)^{3/2}} \qquad (y \geqslant 3)$$

où l'on a posé $\delta := 1 - (1 + \log_2 2)/\log 2 \approx 0.08607$ et où, ici et dans la suite, nous désignons par $\log_k$ la k-ième itérée de la fonction logarithme. Nous renvoyons le lecteur à l'article de synthèse [13] pour une mise en perspective plus complète de ce problème et de ses ramifications.

La valeur de l'exposant δ peut être devinée facilement : la croissance normale des facteurs premiers d'un entier n étant doublement exponentielle (voir par exemple [6] et le chapitre 1 de [8]), on peut approcher, en première analyse, le nombre des diviseurs de n n'excédant pas $2y$ par $2^{\omega(n,y)}$, où $\omega(n, y)$ désigne le nombre des facteurs premiers n'excédant pas y ; si l'on fait l'hypothèse que tous les intervalles dyadiques reçoivent un quota statistique de diviseurs, on est amené à conjecturer que les entiers de $\mathscr{H}_y$ sont caractérisés par la condition $2^{\omega(n,y)} \gg \log y$. Or la densité de l'ensemble des entiers n tels que $\omega(n, y) \geqslant (\log_2 y)/\log 2 + O(1)$ vaut classiquement $1/(\log y)^{\delta+o(1)}$ — voir par exemple [14], ch. II.6.

Nous nous intéressons ici à un phénomène particulier, connu des spécialistes mais qui, à notre connaissance, n'a jamais été clairement mis en évidence dans la littérature : *la structure locale de la suite des facteurs premiers d'un entier est statistiquement gouvernée par son cardinal global*. À l'appui de ce principe, et dans l'intention d'en fournir une illustration emblématique, nous nous proposons d'examiner la probabilité conditionnelle pour qu'un entier n ayant k facteurs premiers possède un diviseur dans un intervalle $]y, 2y]$ donné. Conformément à l'heuristique développée plus haut, la conclusion qualitative de nos résultats est que cette probabilité est minorée par une constante positive lorsque $\omega(n) := \omega(n, n)$ dépasse sensiblement $(\log_2 n)/\log 2$ alors qu'elle tend vers 0 dans le cas contraire.

Désignons par $\mathscr{E}_k(x)$ l'ensemble des entiers $n \leqslant x$ tels que $\omega(n) = k$, par $\pi_k(x)$ son cardinal, et par $H_k(x, y)$ le nombre des entiers n de $\mathscr{E}_k(x)$ qui ont au moins un diviseur dans $]y, 2y]$. Nos résultats sont contenus dans les deux énoncés suivants.

Théorème 1.1 *Soient $R > 0$, $\beta > 1/\log 2$. Il existe des constantes positives c, K, dépendant au plus de R et β, telles que l'on ait*

$$c\pi_k(x) \leqslant H_k(x, y) \leqslant (1 - c)\pi_k(x), \tag{1.1}$$

uniformément pour $2 \leqslant y \leqslant x^{1/K}$, $\beta \log_2 x \leqslant k \leqslant R \log_2 x$. De plus, l'inégalité de droite est valable pour $1 \leqslant k \leqslant R \log_2 x$.

Cet énoncé induit deux questions naturelles, sur lesquelles nous espérons revenir dans un prochain travail :

(a) est-il possible de remplacer, dans les hypothèses, la constante β par une quantité tendant vers $1/\log 2$?
(b) l'encadrement (1.1) est-il valable pour de plus grandes valeurs de k, par exemple $R \log_2 x < k \leqslant (\log x)^{1-\varepsilon}$?

Comme annoncé, la valeur $1/\log 2$ est critique pour la minoration de (1.1). Dans toute la suite, nous utilisons les notations

$$u := \frac{\log x}{\log y}, \qquad \mathfrak{g}(x, y) := \sqrt{\frac{\log u}{(\log_2 y)\log_2 x}} \quad (x \geqslant y \geqslant 3) \tag{1.2}$$

Théorème 1.2 *Soit $\xi(x) \to \infty$. Sous les conditions*

$$\xi(x) \leqslant y \leqslant \sqrt{x}, \qquad k \leqslant \frac{\log_2 x}{\log 2}\big\{1 - \xi(x)\mathfrak{g}(x, y)\big\}, \tag{1.3}$$

nous avons uniformément

$$H_k(x, y) = o\big(\pi_k(x)\big). \tag{1.4}$$

Remarques.

(i) Nous avons

$$\frac{1/\sqrt{2} + o(1)}{\log_2 x} \leqslant \mathfrak{g}(x, y) \leqslant \frac{1}{\sqrt{\log_2 y}}$$

dans le domaine (1.3).

(ii) Des majorations effectives de $H_k(x,y)$ peuvent être aisément déduites de la démonstration donnée au paragraphe 5. Nous nous sommes cantonnés ici à dégager le phénomène qualitatif.

2 Répartition des diviseurs des entiers de $\mathscr{E}_k(x)$

Le résultat suivant fait l'objet du lemme 1 de [12].

Lemme 2.1 *Soient $A > 0$, $B > 0$, et f une fonction arithmétique multiplicative positive ou nulle telle que*

$$\sum_{p^\nu \leqslant x} f(p^\nu)\log p^\nu \leqslant Ax \qquad (x \geqslant 2), \qquad \sum_p \sum_{\nu \geqslant 2} \frac{f(p^\nu)}{p^\nu} \leqslant B.$$

Alors on a, uniformément pour $k \geqslant 1$, $x \geqslant 2$,

$$\sum_{n \in \mathscr{E}_k(x)} f(n) \ll \frac{Ax}{\log x} \frac{\big(\sum_{p \leqslant x} f(p)/p + B\big)^{k-1}}{(k-1)!}, \tag{2.1}$$

où la constante implicite est absolue. En particulier, pour toute constante $R > 0$, nous avons, uniformément sous la condition $1 \leqslant k \leqslant R\log_2 x$,

$$\sum_{n \in \mathscr{E}_k(x)} f(n) \ll \pi_k(x) \exp\Big\{\varrho \sum_{p \leqslant x} \frac{f(p)-1}{p}\Big\} \tag{2.2}$$

avec $\varrho := (k-1)/\log_2 x$ et où la constante implicite dépend au plus de A, B, R.

Dans toute la suite, nous nous donnons des paramètres $x \geqslant 2$, $y \in [2, \sqrt{x}]$, et $L \in [1, \log_2 y]$. Soit $\mathfrak{s}_L := \exp\exp L$ ($L > 0$). Pour chaque entier n, nous écrivons

$$n_L := \prod_{\substack{p \leqslant \mathfrak{s}_L \\ p^\nu \| n}} p^\nu.$$

Enfin, il est commode d'introduire la fonction $Q : \mathbb{R}^+ \to \mathbb{R}^+$ définie par

$$Q(\alpha) := \alpha\log\alpha - \alpha + 1.$$

Notons que $Q(\alpha) \geqslant 0$ avec égalité si, et seulement si, $\alpha = 1$.

Lemme 2.2 *Soient $R > 0$, $x \geqslant 3$ et $1 \leqslant k \leqslant R\log_2 x$. Posant*

$$L_1 := \min(L, \log_2 x - L) \tag{2.3}$$

et définissant implicitement $\kappa \in]0, R]$ *par* $k = \kappa \log_2 x$, *nous avons, uniformément pour* $1 \leqslant L \leqslant \log_2 x$, $1 \leqslant \xi \leqslant \sqrt{L_1}$,

$$\left|\left\{n \in \mathscr{E}_k(x) : |\omega(n_L) - \kappa L| > \kappa\xi\sqrt{L_1}\right\}\right| \ll_R \pi_k(x)\mathrm{e}^{-\kappa\xi^2/3}, \tag{2.4}$$

où l'on peut remplacer $\xi^2/3$ *par* $\xi^2/2$ *si* $\xi \leqslant L_1^{1/6}$.

Démonstration. Supposons dans un premier temps que $L \leqslant \frac{1}{2}\log_2 x$, et donc $L_1 = L$. Posons $s_1 = 1 - \xi/\sqrt{L_1}$, $s_2 = 1 + \xi/\sqrt{L_1}$. Le cardinal à majorer n'excède pas

$$\sum_{1\leqslant j\leqslant 2}\sum_{n\leqslant x} s_j^{\omega(n_L)-s_j\kappa L} \ll \pi_k(x)\left\{\mathrm{e}^{-\kappa Q(s_1)L} + \mathrm{e}^{-\kappa Q(s_2)L}\right\} \ll \pi_k(x)\mathrm{e}^{-\kappa\xi^2/3},$$

où la première estimation découle du Lemme 2.1 et la seconde de l'évaluation

$$\tfrac{1}{3}s^2 \leqslant Q(1+s) \leqslant \tfrac{1}{2}s^2 \leqslant Q(1-s) \qquad (0 \leqslant s \leqslant 1).$$

L'assertion relative au cas $\xi \leqslant L^{1/6}$ résulte du développement

$$Q(1+s) = \tfrac{1}{2}s^2 + O(s^3)$$

au voisinage de $s = 0$.

Lorsque $L > \frac{1}{2}\log_2 x$, et donc $L_1 = \log_2 x - L$, nous observons que la condition sur $\omega(n_L)$ apparaissant dans (2.4) équivaut à $|\omega(n) - \omega(n_L) - (k - \kappa L)| > \kappa\xi\sqrt{L_1}$. On peut alors procéder similairement au cas précédent, en considérant les facteurs premiers de $]\mathfrak{s}_L, x]$. □

Lemme 2.3 *Soit* $R > 0$, $x \geqslant 3$ *et* $1 \leqslant k \leqslant R\log_2 x$. *On définit implicitement* $\kappa \in]0, R]$ *par* $k = \kappa \log_2 x$. *Nous avons, uniformément pour* $1 \leqslant L \leqslant \log_2 x$, $T > 0$,

$$\left|\left\{n \in \mathscr{E}_k(x) : \log n_L > T\mathrm{e}^L\right\}\right| \ll \pi_k(x)\mathrm{e}^{-T/2}.$$

Démonstration. Nous pouvons supposer L assez grand puisque le résultat est trivial lorsque L est borné. Posons $\alpha := \frac{1}{2}\mathrm{e}^{-L}$. Alors la fonction $n \mapsto n_L^\alpha$ est multiplicative et, puisque $\sqrt{\mathrm{e}} < 2$, satisfait les hypothèses du Lemme 2.1 pour des constantes absolues convenables A et B. La quantité à estimer n'excède pas

$$\sum_{n\in\mathscr{E}_k(x)} \left\{n_L/\exp\left(T\mathrm{e}^L\right)\right\}^\alpha = \mathrm{e}^{-T/2}\sum_{n\in\mathscr{E}_k(x)} n_L^\alpha.$$

Le Lemme 2.1 fournit aisément que la dernière somme est $\ll \pi_k(x)$. L'estimation souhaitée en résulte. □

Nous posons encore

$$\omega_\vartheta(m) := \sum_{p\mid m,\, p\leqslant \exp(1/|\vartheta|)} 1 \quad (m\geqslant 1,\ \vartheta\neq 0),$$

$$\omega(n;s,t) := \sum_{p\mid n,\, s<\log_2 p\leqslant t} 1 \qquad (0<s\leqslant t),$$

$$\sigma(t) := t-\sqrt{t\log t} \qquad (t>1).$$

Le résultat suivant est énoncé, à fins d'applications ultérieures, sous une forme significativement plus précise que nécessaire pour le présent travail.

Lemme 2.4 *Soient $R>0$, $\varepsilon\in]0,\frac12]$, $x\geqslant 3$, $1\leqslant k\leqslant R\log_2 x$, $1\leqslant L\leqslant \log_2 x$. On définit implicitement $\kappa\in]0,R]$ par $k=\kappa\log_2 x$. Nous avons*

$$\min_{1/(\varepsilon\mathrm{e}^L)\leqslant|\vartheta|\leqslant 2} \frac{\omega(n_L)-\omega_\vartheta(n_L)}{\sigma(L+\log|\vartheta|)} > \kappa \tag{2.5}$$

pour tous les entiers n de $\mathscr{E}_k(x)$ sauf au plus $\ll \pi_k(x)/\{\log(1/\varepsilon)\}^{1/4}$. La constante implicite dépend au plus de R.

Démonstration. Considérons un entier n contrevenant à (2.5). Il existe alors $\vartheta\in]1/(\varepsilon\mathrm{e}^L),2]$ tel que, posant $j_\vartheta := \lfloor L+\log|\vartheta|\rfloor$, et donc $j_\vartheta>\log(1/\varepsilon)-1$, l'on puisse écrire, pour tout $v\in]0,1]$,

$$1\leqslant v^{\omega_\vartheta(n_L)-\omega(n_L)-\kappa\sigma(j_\vartheta)} < v^{-\kappa-\kappa(j_\vartheta)} v^{\omega(n;L-j_\vartheta,L)}.$$

Ainsi, le nombre R_x des entiers exceptionnels satisfait

$$R_x \leqslant \sum_{\log(1/\varepsilon)-1<j\leqslant L} v_j^{-\kappa\{1+\sigma(j)\}} \sum_{n\in\mathscr{E}_k(x)} v_j^{\omega(n;L-j,L)},$$

pour tout choix de $v_j\in]0,1]$. Nous pouvons employer Lemme 2.1 pour majorer la somme intérieure. Elle est

$$\ll \pi_k(x)\mathrm{e}^{-\kappa(1-v_j)j}.$$

Pour le choix $v_j := 1-\sqrt{(\log j)/j}$, nous obtenons que le facteur sommé dépendant de j est $\ll \pi_k(x)j^{-5/4}$. Il suit

$$R_x \ll \sum_{j>\log(1/\varepsilon)-1} \frac{\pi_k(x)}{j^{5/4}} \ll \frac{\pi_k(x)}{\{\log(1/\varepsilon)\}^{1/4}}. \qquad \square$$

Soit $\mathscr{L}(m) := \cup_{d|m}\big(\log d + \big[-\frac{1}{2}, 0\big[\big)$. Nous désignons par $\lambda(m)$ la mesure de Lebesgue de $\mathscr{L}(m)$ et posons

$$\tau(m, \vartheta) := \sum_{d|m} d^{i\vartheta} \qquad (m \in \mathbb{N}^*,\ \vartheta \in \mathbb{R}).$$

Le résultat suivant a été établi dans [11].

Lemme 2.5 *Pour chaque entier naturel m, nous avons*

$$\lambda(m) \int_{-2}^{2} \frac{|\tau(m, \vartheta)|^2}{\tau(m)^2} \mathrm{d}\vartheta \geqslant \frac{1}{3\pi}. \tag{2.6}$$

Lemme 2.6 *Soit $R > 0$. Nous avons, uniformément pour $x \geqslant 3$, $1 \leqslant k \leqslant R \log_2 x$ et $\vartheta \in \mathbb{R}^*$,*

$$\sum_{n \in \mathscr{E}_k(x)} \frac{|\tau(n_L, \vartheta)|^2}{2^{\omega(n_L)+\omega_\vartheta(n_L)}} \ll \pi_k(x)\{\log(3 + |\vartheta|)\}^{2\kappa}. \tag{2.7}$$

Démonstration. Appliquons à nouveau le Lemme 2.1. Le membre de gauche de (2.7) est

$$\ll \pi_k(x) \exp\left\{\kappa \sum_{\log(1/|\vartheta|) < \log_2 p \leqslant L} \frac{\cos(\vartheta \log p)}{p}\right\}.$$

La somme en p peut être estimée par sommation d'Abel à l'aide du théorème des nombres premiers, comme au lemme III.4.13 de [14]. En estimant trivialement la contribution éventuelle des nombres premiers p tels que

$$\exp(1/|\vartheta|) < p \leqslant \exp\{\log^2(3 + |\vartheta|)\},$$

nous obtenons qu'elle n'excède pas $2\log_2(3 + |\vartheta|) + O(1)$. Cela fournit bien (2.7). □

Lemme 2.7 *Soient $R > 0$, $\beta > 1/\log 2$, $\delta := \beta \log 2 - 1$. Pour tous $x \geqslant 2$, $\varepsilon > 0$, $k \in \mathbb{N}$, tels que*

$$\beta \log_2 x \leqslant k \leqslant R \log_2 x,$$

le nombre $M_k(x; \varepsilon)$ des entiers n de $\mathscr{E}_k(x)$ tels que $\lambda(n_L) \leqslant \varepsilon \mathrm{e}^L$ satisfait

$$M_k(x; \varepsilon) \ll \pi_k(x)\Big\{\varepsilon^{\delta/2} + \varepsilon^{\kappa Q(1-\delta/3)}\Big\}. \tag{2.8}$$

La constante implicite dépend au plus de R et β.

Démonstration. D'après (2.6), un entier n compté dans $M_k(x;\varepsilon)$ satisfait nécessairement

$$3\pi\varepsilon \mathrm{e}^L \int_{-2}^{2} \frac{|\tau(n_L,\vartheta)|^2}{\tau(n_L)^2}\mathrm{d}\vartheta \geqslant 1.$$

Comme la contribution à l'intégrale des nombres réels ϑ tels que $|\vartheta| \leqslant \mathrm{e}^{-L}/(12\pi\varepsilon)$ est trivialement $\leqslant \frac{1}{2}$, il suit

$$\varepsilon_1 \mathrm{e}^L \int_{\mathrm{e}^{-L}/\varepsilon_1}^{2} \frac{|\tau(n_L,\vartheta)|^2}{\tau(n_L)^2}\mathrm{d}\vartheta \geqslant 1, \tag{2.9}$$

où, pour simplifier l'écriture, nous avons posé $\varepsilon_1 := 12\pi\varepsilon$.

Maintenant, nous observons que, quitte à écarter un ensemble d'entiers n de cardinal majoré par le membre de gauche de (2.8), le Lemme 2.4 nous permet de supposer que

$$\min_{1/(\varepsilon_1\mathrm{e}^L)\leqslant|\vartheta|\leqslant 2} \frac{\omega(n_L)-\omega_\vartheta(n_L)}{L+\log|\vartheta|} > \frac{1+\delta/2}{\log 2},$$

et donc

$$2^{\omega(n_L)-\omega_\vartheta(n_L)} > (\vartheta \mathrm{e}^L)^{1+\delta/2}.$$

Cela implique

$$\int_{\mathrm{e}^{-L}/\varepsilon_1}^{2} \frac{|\tau(n_L,\vartheta)|^2}{\tau(n_L)^2}\mathrm{d}\vartheta \geq \int_{\mathrm{e}^{-L}/\varepsilon_1}^{2} \frac{|\tau(n_L,\vartheta)|^2}{2^{\omega(n_L)+\omega_\vartheta(n_L)}} \frac{\mathrm{d}\vartheta}{(\vartheta\mathrm{e}^L)^{1+\delta/2}}.$$

En tenant compte de (2.9), nous obtenons

$$\begin{aligned} M_k(x;\varepsilon) &\leqslant \varepsilon_1 \int_{\mathrm{e}^{-L}/\varepsilon_1}^{2} \sum_{\substack{n\leqslant x\\ \omega(n)=k}} \frac{|\tau(n_L,\vartheta)|^2}{2^{\omega(n_L)+\omega_\vartheta(n_L)}} \frac{\mathrm{d}(\vartheta\mathrm{e}^L)}{(\vartheta\mathrm{e}^L)^{1+\delta/2}} + O\big(\pi_k(x)\varepsilon^{\kappa Q(\alpha)}\big) \\ &\ll \pi_k(x)\big\{\varepsilon^{\delta/2} + \varepsilon^{\kappa Q(\alpha)}\big\}, \end{aligned}$$

d'après le Lemme 2.6. □

3 Entiers de $\mathscr{E}_k(x)$ sans petit facteur premier

Désignons par $P^-(n)$ (resp. $P^+(n)$) le plus petit (resp. le plus grand) facteur premier d'un entier générique $n > 1$ avec la convention $P^-(1) = \infty$ (resp. $P^+(1) = 1$). Nous posons alors

$$\pi_k(x, y) := \big|\{n \in \mathscr{E}_k(x) : P^-(n) > y\}\big|.$$

Dans toute cette section, nous notons systématiquement $x = y^u$ lorsque $2 \leqslant y \leqslant x$.

Le résultat suivant a été établi dans [9] (lemme 3.2) comme conséquence très affaiblie de formules asymptotiques dues à Balazard [2] (lemme 5) et Alladi [1] (théorème 7).

Lemme 3.1 *Soit $R > 0$. Il existe $u_0 = u_0(R) > 1$ tel que l'on ait uniformément pour $u \geqslant u_0(R)$, $1 \leqslant k \leqslant R \log u$,*

$$\pi_k(x, y) \asymp \frac{x}{\log x} \frac{(\log u)^{k-1}}{(k-1)!}. \tag{3.1}$$

Lemme 3.2 *Soient c_1, c_2 des constantes telles que $0 < c_1 < c_2$. Il existe $\varepsilon_1 = \varepsilon_1(c_1, c_2) > 0$ tel que l'on ait, uniformément pour $1 \leqslant z^{c_1} \leqslant y \leqslant z \leqslant x^{\varepsilon_1}$, $1 \leqslant d \leqslant \sqrt{x}$, et $c_1 \log u \leqslant k \leqslant c_2 \log u$,*

$$\pi_{k-1}(x/d, z) \asymp \pi_k(x, y)/d. \tag{3.2}$$

Démonstration. Cela résulte immédiatement de (3.1).

4 Preuve du Théorème 1.1

Commençons par établir la minoration. Nous retenons la notation $\kappa := k/\log_2 x$ introduite précédemment.

Nous pouvons supposer $y \geqslant y_0$ où y_0 est une constante arbitrairement choisie. En effet, dans le cas contraire, on a $H_k(x, y) \geqslant \pi_{k-\omega(m)}(x/m, y) \gg \pi_k(x, y)$ avec, par exemple, $m = 1 + \lfloor y \rfloor \in]y, 2y]$.

Soit ε une constante absolue positive assez petite, dont nous préciserons la valeur ultérieurement. Nous posons $L := \log_2 y^\varepsilon$, conservons la notation (2.3), et considérons l'ensemble

$$\mathfrak{M} := \left\{ m \leqslant \sqrt{y} : \begin{array}{c} P^+(m) \leqslant y^\varepsilon,\ |\omega(m) - \kappa L| \leqslant \sqrt{L_1} \log\left(\dfrac{1}{\varepsilon}\right), \\ \tau(m) \leqslant 3^L, \lambda(m) > \varepsilon \mathrm{e}^L \end{array} \right\}.$$

Les Lemmes 2.2, 2.3 et 2.7 garantissent que, pour ε convenablement choisi, $x > x_0(\varepsilon)$, et $K = K(\varepsilon)$ assez grand, on a $n_L \in \mathfrak{M}$ pour au moins $\frac{1}{2}\pi_k(x)$ entiers n de $\mathscr{E}_k(x)$. En décomposant chacun de ces entiers sous la forme mh avec $P^-(h) > y^\varepsilon$, il suit

$$\tfrac{1}{2}\pi_k(x) \leqslant \sum_{m\in\mathfrak{M}} \pi_{k-\omega(m)}(x/m, y^\varepsilon). \tag{4.1}$$

Considérons alors les entiers n de $\mathscr{E}_k(x)$ qui peuvent s'écrire sous la forme mph avec $m \in \mathfrak{M}$, $\log y - \log p \in \mathscr{L}(m)$, $P^-(h) > 2y$. La seconde condition implique l'existence d'un diviseur d de m tel que

$$\log d - \tfrac{1}{2} \leqslant \log y - \log p < \log d$$

donc $dp \in]y, 2y]$. Comme on a nécessairement

$$\log p > \log y - \log m \geqslant \tfrac{1}{2}\log y > \log y^\varepsilon,$$

la décomposition $n = mph$, lorsqu'elle existe, est unique.

Posant $\mathscr{G}(y,m) := \{t \in \mathbb{R}^+ : \log(y/t) \in \mathscr{L}(m)\}$, nous pouvons donc écrire

$$H_k(x,y) \geq \sum_{m\in\mathfrak{M}} \sum_{p\in\mathscr{G}(y,m)} \pi_{k-1-\omega(m)}(x/pm, 2y). \tag{4.2}$$

Notant à présent $u := (\log x)/\log 2y$, nous avons

$$k - \omega(m) = k - \kappa L + O_\varepsilon\big(\sqrt{L_1}\big) = \kappa \log u + O_\varepsilon\big(\sqrt{L_1}\big),$$

d'après la définition de $\mathfrak{M}$. Lorsque $y \leqslant x^{1/K}$, où $K = K(\varepsilon)$ est une constante convenable, cela implique $k - \omega(m) \asymp \log u$. Nous sommes donc en mesure d'appliquer le Lemme 3.2 avec $d = p$ pour déduire que, pour tous les couples (m,p) de la sommation de (4.2), nous avons

$$\pi_{k-1-\omega(m)}(x/pm, 2y) \asymp_\varepsilon \pi_{k-\omega(m)}(x/m, y^\varepsilon)/p.$$

À ce stade, nous observons que $\mathscr{G}(y,m)$ est, pour chaque $m \in \mathfrak{M}$, une réunion d'au plus $\tau(m) \leqslant (\log y)^2$ intervalles de longueur logarithmique totale $\lambda(m)$ et dont les bornes ont des logarithmes de l'ordre de $\log y$. Nous avons donc

$$\sum_{p\in\mathscr{G}(y,m)} \frac{1}{p} \gg \frac{1}{\log y} \sum_{p\in\mathscr{G}(y,m)} \frac{\log p}{p} \gg \frac{\lambda(m)}{\log y} + O\bigg(\frac{\log y}{\mathrm{e}^{\sqrt{\log y}}}\bigg) \gg 1.$$

En reportant dans (4.2), il suit

$$H_k(x,y) \gg_\varepsilon \sum_{m\in\mathfrak{M}} \pi_{k-\omega(m)}\Big(\frac{x}{m}, y^\varepsilon\Big) \sum_{p\in\mathscr{G}(y,m)} \frac{1}{p} \gg \sum_{m\in\mathfrak{M}} \pi_{k-\omega(m)}\Big(\frac{x}{m}, y^\varepsilon\Big) \gg \pi_k(x),$$

où la dernière minoration résulte de (4.1). Établissons maintenant la majoration de (1.1). À cette fin, nous considérons le nombre $J_k(x,y)$ des entiers n de $\mathscr{E}_k(x)$ tels que $n_L \leqslant y$, avec à présent $L := \log_2 2y$. Nous avons évidemment

$$\pi_k(x) - H_k(x,y) \geqslant J_k(x,y).$$

Nous allons montrer que

$$J_k(x,y) \gg \pi_k(x). \tag{4.3}$$

Chaque entier de la forme $n = mh$ avec $m \leqslant y$, $P^-(h) > 2y$ et $\omega(m) + \omega(h) = k$ est compté dans $J_k(x,y)$. On peut donc écrire

$$J_k(x,y) \geqslant \sum_{m\leqslant y} \pi_{k-\omega(m)}(x/m, 2y).$$

Retenons seulement dans la sommation les entiers m tels que

$$|\omega(m) - \kappa L| \leqslant L_1.$$

Nous avons alors $k - \omega(m) \ll \log u = \log_2 x - \log_2 y$ sous l'hypothèse $y \leqslant x^{1/K}$ dès que la constante K est convenablement choisie. Par (3.1) il suit

$$J_k(x,y) \gg \frac{x}{\log x} \sum_{\substack{m\leqslant y\\ |\omega(m)-\kappa L|\leqslant L_1}} \frac{(\log u)^{k-\omega(m)-1}}{(k-\omega(m)-1)!\, m}. \tag{4.4}$$

Une sommation d'Abel permet de déduire des estimations connues de $\pi_k(x)$ (cf., par exemple, [14], chapitre II.6) que l'on a, pour $|j - \kappa L| \leqslant L_1$,

$$\sum_{\substack{m\leqslant y\\ \omega(m)=j}} \frac{1}{m} \asymp_\varepsilon \frac{(\log_2 y)^j}{j!}.$$

En reportant dans (4.4), il suit

$$J_k(x,y) \gg \frac{x}{\log x} \frac{(\log_2 x)^{k-1}}{(k-1)!} \sum_{|j-\kappa L|\leqslant L_1} \binom{k-1}{j} (1-\vartheta)^{k-1-j}\vartheta^j$$

avec $\vartheta := (\log_2 y)/\log_2 x$, de sorte que $\kappa L = k\vartheta$ et, pour un choix convenable des constantes, $L_1 \geqslant 2\sqrt{\vartheta(1-\vartheta)k}$. Un résultat classique sur les sommes partielles du binôme (voir par exemple le théorème 6.1 de [4]) implique que la somme en j est $\gg 1$. Nous obtenons donc (4.3), ce qui achève la démonstration du Théorème 1.1.

5 Preuve du Théorème 1.2

Nous supposons dans toute la suite $y_0 \leqslant y \leqslant \sqrt{x}$, où y_0 désigne une constante assez grande.

Chaque entier n compté dans $H_k(x,y)$ admet une représentation sous la forme $n = md$ avec $d \in]y, 2y]$. Posons alors

$$r = (m,d), \qquad m = m_0 r_1 r, \quad d = d_0 r_2 r, \quad r_1 r_2 \mid r^\infty,$$
$$a = \omega(m_0), \quad b = \omega(d_0), \quad j := a + b \leqslant k,$$

de sorte que $\omega(r) = k - j$.

Il suit

$$H_k(x,y) \leqslant \sum_{\substack{j\leqslant k\\ a+b=j}} \sum_{\substack{r\geqslant 1, r_1\geqslant 1, r_2\geqslant 1\\ r_1r_2\mid r^\infty\\ \omega(r)=k-j}} \sum_{\substack{y/rr_2<d\leqslant 2y/rr_2\\ \omega(d_0)=b}} \sum_{\substack{m_0\leqslant x/d_0r_1r_2r^2\\ \omega(m_0)=a}} 1.$$

On montre facilement que la contribution correspondant à la condition supplémentaire $r_1 r > x^{1/4}$ est $\ll \pi_k(x)/\log x$: en effet, une majoration triviale des sommes en m_0 et d_0 fournit une borne

$$\ll \sum_{\substack{r\geqslant 1, r_1\geqslant 1, r_2\geqslant 1\\ r_1r_2\mid r^\infty\\ x^{1/4}<r_1r\leq x}} \frac{x}{r_1r_2r^2} \ll \sum_{\substack{r\leqslant x\\ r_1r_2\mid r^\infty}} \frac{x^{7/8}}{\sqrt{r_1}r_2r^{3/2}} \ll \sum_{r\geqslant 1} \frac{x^{7/8}}{r\varphi(r)} \prod_{p\mid r}\Big(1-\frac{1}{\sqrt{p}}\Big) \ll x^{7/8}.$$

Lorsque $r_1 r \leqslant x^{1/4}$, des estimations classiques (cf., par exemple, [14], chapitre II.6), impliquent que la double somme intérieure est

$$\ll \frac{x(\log_2 x)^{a-1}(\log_2 y)^{b-1}}{r^2 r_1 r_2 (a-1)!(b-1)!(\log 3y/r)\log x}.$$

Par sommation sur a et b, nous obtenons

$$\begin{aligned} H_k(x,y) &\ll x \sum_{j\leqslant k} \sum_{\substack{r\geqslant 1, r_1\geqslant 1, r_2\geqslant 1\\ r_1r_2\mid r^\infty\\ \omega(r)=k-j}} \frac{(\log_2 x+\log_2 y)^{j-2}}{r^2 r_1 r_2 (j-2)!\log x(\log 3y/r)} \\ &\ll x \sum_{j\leqslant k} \sum_{\substack{r\geqslant 1\\ \omega(r)=k-j}} \frac{(\log_2 x+\log_2 y)^{j-2}}{\phi(r)^2 (j-2)!\log x(\log 3y/r)} \\ &\ll \frac{\pi_k(x)}{\log y}\Big(1+\frac{\log_2 y}{\log_2 x}\Big)^k = \frac{2^k\pi_k(x)}{\log y}\Big(1-\frac{\log u}{2\log_2 x}\Big)^k, \end{aligned}$$

sous l'hypothèse $k \ll \log_2 x$.

Il vient

$$H_k(x,y) \ll \frac{2^k\pi_k(x)u^{-k/2\log_2 x}}{\log y} = \frac{2^k\pi_k(x)u^{1-\kappa/2}}{\log x}$$

où nous avons conservé la notation $\kappa = k/\log_2 x$.

La majoration souhaitée (1.4) est donc acquise dès que

$$k \leqslant \frac{\log_2 x}{\log 2} - \frac{1-1/\log 4}{\log 2}\log u - \xi(x). \tag{5.1}$$

Cela fournit la conclusion annoncée lorsque, disons, $\log y > \mathrm{e}^{-\xi^2}\log x$.

Nous pouvons donc supposer dans la suite que $u > \mathrm{e}^{\xi^2}$. Choisissons $L := \log_2 y$ et conservons la notation (2.3). Nous pouvons supposer sans perte de généralité que la fonction $\xi = \xi(x)$ apparaissant dans l'hypothèse (1.3) satisfait également $\xi \leqslant \sqrt{L_1}$. Soit $\kappa_1 = (1+\xi\sqrt{L_1}/L)\kappa$. En vertu du Lemme 2.2, quitte à écarter un nombre acceptable d'entiers exceptionnels, nous pouvons supposer que

$$\omega(n_L) \leqslant \kappa_1 L. \tag{5.2}$$

De même, nous déduisons du Lemme 2.3 que l'on peut supposer

$$n_L \leqslant x_1 := x^{\exp(-\xi^2/2)}. \tag{5.3}$$

Les entiers restants comptés dans $H_k(x,y)$ admettent une représentation sous la forme $n = dtm$, avec les conditions

$$y < d \leqslant 2y, \quad P^+(t) \leqslant y, \quad t \leqslant x_1, \quad P^-(m) > y.$$

Soit $H_k^*(x,y)$ le nombre de tels entiers n n'excédant pas x et tels que $\omega(n)=k$. Nous avons

$$H_k^*(x,y) \leqslant \sum_{j\leqslant \kappa_1 L} \sum_{y<d\leqslant 2y} \sum_{\substack{t\leqslant x_1\\ P^+(t)\leqslant y\\ \omega(dt)=j}} \sum_{\substack{m\leqslant x/dt\\ \omega(m)=k-j\\ P^-(m)>y}} 1.$$

La somme intérieure relève du Lemme 2.1. Elle est

$$\ll \frac{x}{dt\log x}\frac{(\log_2 x-\log_2 y+B)^{k-j-1}}{(k-j-1)!},$$

où B est une constante absolue convenable. Posons alors $d=rd_1$, $t=rt_1$, avec $(d_1,t_1)=1$. Nous avons $\omega(d_1)+\omega(t_1)\leqslant j$, donc

$$\begin{aligned}\sum_{y<d\leqslant 2y}\sum_{\substack{t\leqslant x_1\\ P^+(t)\leqslant y\\ \omega(dt)=j}}\frac{1}{dt} &\ll \sum_{r\leqslant 2y}\frac{1}{r^2}\sum_{a+b\leqslant j}\sum_{\substack{y/r<d_1\leqslant 2y/r\\ \omega(d_1)=a}}\frac{1}{d_1}\sum_{\substack{t_1\leqslant x_1\\ \omega(t_1)=b}}\frac{1}{t_1}\\ &\ll \sum_{r\leqslant 2y}\frac{1}{r^2}\sum_{a+b\leqslant j}\frac{(\log_2 y)^{a+b-1}}{(a-1)!b!(\log 3y/r)} \ll \sum_{r\leqslant 2y}\frac{1}{r^2}\sum_{c\leqslant j-1}\frac{(2\log_2 y)^c}{c!\log(3y/r)}\\ &\ll \frac{1}{\log y}\sum_{c\leqslant j}\frac{(2\log_2 y)^c}{c!} \ll \frac{(2\log_2 y)^j}{j!\log y}.\end{aligned}$$

Nous avons utilisé ici les estimations classiques de $\pi_\ell(v)$ pour estimer les sommes en d_1 et t_1. Pour la dernière majoration, nous avons fait appel au résultat bien connu stipulant que, puisque $j\leq \kappa_1\log_2 y$ avec $\kappa_1\leqslant 1/\log 2<2$, la dernière somme en c est dominée par le terme d'indice $c=j$.

Il suit finalement

$$\begin{aligned}H_k^*(x,y) &\ll \frac{x}{(\log x)\log y}\sum_{j\leqslant \kappa_1 L}\frac{(2\log_2 y)^j}{j!}\frac{(\log_2 x-\log_2 y+B)^{k-j-1}}{(k-j-1)!}\\ &\ll \frac{x2^{\kappa_1\log_2 y}}{(\log x)\log y}\sum_{j\leqslant k}\frac{(\log_2 y)^j}{j!}\frac{(\log_2 x-\log_2 y+B)^{k-j-1}}{(k-j-1)!}\\ &\ll \pi_k(x)(\log y)^{\kappa_1\log 2-1}.\end{aligned}$$

On vérifie alors que $(\log y)^{\kappa_1\log 2-1}$ tend vers 0 dès que

$$k\leqslant \frac{\log_2 x}{\log 2}\left(1-\frac{\xi\sqrt{L_1}}{L\log 4}\right).$$

Comme

$$\sqrt{\frac{L_1}{L}} \asymp \sqrt{\frac{\log u}{(\log_2 y)\log_2 x}} = \mathfrak{g}(x, y),$$

nous obtenons le résultat souhaité, quitte à altérer la fonction arbitraire ξ.

References

1. K. Alladi, The distribution of $\nu(n)$ in the sieve of Eratosthenes. Q. J. Math. **33**(2), 129–148 (1982)
2. M. Balazard, Unimodalité de la distribution du nombre de diviseurs premiers d'un entier. Ann. Inst. Fourier Grenoble **40**(2), 255–270 (1990)
3. A.S. Besicovitch, On the density of certain sequences. Math. Ann. **110**, 336–341 (1934)
4. C. Dartyge, G. Tenenbaum, Sommes des chiffres de multiples d'entiers. Ann. Inst. Fourier Grenoble **55**(7), 2423–2474 (2005)
5. P. Erdős, A generalization of a theorem of Besicovitch. J. Lond. Math. Soc. **11**, 92–98 (1936)
6. P. Erdős, On the distribution function of additive functions. Ann. Math. **47**, 1–20 (1946)
7. K. Ford, The distribution of integers with a divisor in a given interval. Ann. Math. (2) **168**(2), 367–433 (2008)
8. R.R. Hall, G. Tenenbaum, *Divisors*. Cambridge Tracts in Mathematics, vol. 90 (Cambridge University Press, Cambridge, 1988), paperback ed. (2008)
9. A. Raouj, A. Stef, G. Tenenbaum, Mesures quadratiques de la proximité des diviseurs. Math. Proc. Camb. Philos. Soc. **150**, 73–96 (2011)
10. G. Tenenbaum, Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné. Compos. Math. **51**, 243–263 (1984)
11. G. Tenenbaum, Sur une question d'Erdős et Schinzel, in *A Tribute to Paul Erdős,* ed. by A. Baker, B. Bollobás, A. Hajnal (Cambridge University Press, Cambridge, 1990), pp. 405–443
12. G. Tenenbaum, A rate estimate in Billingsley's theorem for the size distribution of large prime factors. Q. J. Math. **51**, 385–403 (2000)
13. G. Tenenbaum, Some of Erdős' unconventional problems in number theory, thirty-four years later, in *Erdős Centennial Volume*, ed. by L. Lovász, I.Z. Ruzsa, V.T. Sós. Bolyai Society Mathematical Studies, vol. 25 (Springer, Heidelberg, 2013), pp. 651–681
14. G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 4-ième éd., coll. Échelles, Belin, 2015, 592 pp. English translation: Graduates Studies in Mathematics, vol. 163 (Amer. Math. Soc., 2015)

A Ternary Problem in Additive Prime Number Theory

Jörg Brüdern

Abstract Estimates are obtained for the number of natural numbers below a parameter that do not have a representation as the sum of two squares of primes and a kth power of a prime. These improve earlier bounds in the order of magnitude. The method is then also applied to some related questions.

Keywords Circle method • Sums of prime powers

2010 Mathematics subject classification: Primary 11P32; Secondary 11P55

1 Introduction

This collection of research articles is dedicated to the memory of Wolfgang Schwarz. Early in his career he was a practitioner of the Hardy–Littlewood circle method [14–16], and he followed later developments of the method itself and its range of applicability with great interest. His survey article [17] gives ample proof of this, and the collection of open problems contained therein helped this writer into the subject [1]. It therefore seems fitting for the occasion to examine here the current status of a problem that Schwarz discussed in his thesis. Published in two parts [14, 15] and devoted in general to the additive theory of prime numbers, it is in the second of his papers where the intent is to obtain proof that almost all numbers expected to be representable in a certain proposed form indeed have such representations.

Perhaps the most interesting of his results relates to representations of the natural number n in the form

$$n = p_2^2 + p_2^2 + p_3^k \tag{1.1}$$

J. Brüdern (✉)
Mathematisches Institut, Bunsenstrasse 3-5, 37073 Göttingen, Germany
e-mail: bruedern@uni-math.gwdg.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_4

in which $k \geq 2$ is a given natural number, and the variables p_j range over primes. One may expect such a representation to exist whenever the congruences

$$x_1^2 + x_2^2 + x_3^k \equiv n \bmod q \tag{1.2}$$

are soluble with $(x_j, q) = 1$ $(1 \leq j \leq 3)$, for all $q \in \mathbb{N}$, and we write $\mathscr{H}_k$ for the set of all $n \in \mathbb{N}$ where this is so. It is well known and easy to prove[1] that $\mathscr{H}_k$ is the union of finitely many residue classes. In particular, $\mathscr{H}_k$ has positive density among the natural numbers. Schwarz [15, Satz 3] proved that for any fixed $A > 0$ the number $E_k(N)$ of integers $n \in \mathscr{H}_k$ with $1 \leq n \leq N$ for which (1.1) has no solution in primes p_1, p_2, p_3 satisfies $E_k(N) \ll N(\log N)^{-A}$. Earlier Hua [7] had obtained this same conclusion for *some* positive A. After the fundamental innovations of Montgomery and Vaughan [13] in their treatment of the binary Goldbach problem, an estimate of the shape

$$E_k(N) \ll N^{1-\delta(k)} \tag{1.3}$$

should have been within reach for some positive $\delta(k)$, but a proof was only published in 1993 by Leung and Liu [9]. Their argument relied on the Deuring–Heilbronn phenomenon, as did the work of Montgomery and Vaughan, and hence little could be said about the dependence of δ on k at the time. Five years later Liu and Zhan [11] noticed that for representation problems with more than two variables, potential Siegel zeros impact the major arc analysis to a lesser extent than is the case in a binary situation. This interesting observation has been instrumental in many applications since. In particular, dramatic progress was possible with the quadratic case of the Waring–Goldbach problem. We only mention the latest bound

$$E_2(N) \ll N^{17/20+\varepsilon}$$

due to Harman and Kumchev [5]. For larger values of k, we have (1.3) with

$$\delta(3) = \frac{1}{21} - \varepsilon, \quad \delta(k) = \frac{1}{3k \cdot 2^{k-2}} - \varepsilon \quad (k \geq 4) \tag{1.4}$$

where ε is any positive number, as established by Lü [12] and Li [10, Theorem 1], respectively. These two papers are based on very similar ideas. An elementary bound for the number of solutions of the equation

$$p_1^2 + p_2^2 = p_3^2 + p_4^2$$

in primes p_j not exceeding $N^{1/2}$ is combined with an estimate of Weyl's type for the degree k Weyl sum in a circle method analysis of the problem at hand. When

[1] For details see, for example, the footnote on p. 41 of [3], or *inter alia* in [15].

$k \geq 3$, the best known Weyl bounds for trigonometric sums over prime powers are due to Kumchev [8], and their direct use produces the estimates (1.4). For larger values of k, Li's results can be improved by using Weyl bounds stemming from Vinogradov's mean value theorem. Wooley's groundbreaking work [19] on the latter can be combined with the strategy of Li to show that in (1.3) one may take $\delta(k) = c/k^3$, for some constant $c > 0$.

In this paper we follow a different route and treat the kth power in mean. This increases the admissible values for $\delta(k)$ by a factor k when k is large, and when $k = 3$ we also obtain a sizeable improvement over the work of Lü [12].

Theorem 1.1 *One has*

$$E_3(N) \ll N^{15/16+\varepsilon} \quad \text{and} \quad E_k(N) \ll N^{1-1/(2k)^2+\varepsilon} \quad (k \geq 4).$$

To access the strength of this result, it is perhaps worth pointing out that the circle method approach to problems of this type is currently limited by the square root cancellation barrier. For the problem under consideration, this corresponds to $\delta(k) = 1/k$ in (1.3). If one is prepared to give up the primality of p_3 in (1.1), then one can get reasonably close to this barrier. More precisely, let $\mathscr{G}_k$ be the set of all natural numbers n for which the congruences (1.2) are soluble with $(x_1x_2, q) = 1$, for all $q \in \mathbb{N}$. Let $E_k^*(N)$ denote the number of all $n \in \mathscr{G}_k$ with $1 \leq n \leq N$ for which the equation

$$p_1^2 + p_2^2 + x^k = n \tag{1.5}$$

has no solution in primes p_1, p_2 and natural numbers x.

Theorem 1.2 *Let $k \geq 4$. Then $E_k^*(N) \ll N^{1-1/(97k)}$.*

No effort has been made to optimize the constant 97 that occurs in the exponent of the bound for $E_k^*(N)$. Emphasis is on larger k, and consequently, we have not attempted to tune our approach so as to yield good bounds when k is of moderate size.

It is interesting to compare the conclusion of Theorem 1.2 with related estimates for the prominent Hardy–Littlewood problem concerning sums of a prime and a kth power. When $n \in \mathscr{G}_k$ we expect Eq. (1.5) to have about $n^{1/k}(\log n)^{-2}$ solutions, while whenever $n - x^k$ is irreducible as a polynomial over the rationals, the equation $n = p + x^k$ should have about $n^{1/k}(\log n)^{-1}$ solutions with p prime. Thus, one might be led to believe that the two problems are roughly of the same degree of difficulty. However, this does not seem to be the case, given our current understanding of exponential sums over primes. Indeed, if $D_k(N)$ denotes the number of all $n \leq N$ for which $n - x^k$ is irreducible over $\mathbb{Z}[x]$ but $n = p + x^k$ has no solution with p prime, then the bound

$$D_k(N) \ll N^{1-1/(25k)} \tag{1.6}$$

was obtained in collaboration with Perelli [4] almost 20 years ago, yet assuming that no Dirichlet L-function has a zero in the half-plane Re $s > \frac{1}{2}$. Unconditional bounds for $D_k(N)$ come nowhere close to (1.6). The significant difference between the Hardy–Littlewood problem and the representation problem (1.1) is that the major arc estimates of Kumchev [8] have an amplifying effect whenever three summands are present, but only then. Kumchev's bounds control Weyl sums related to $p_1^2 + p_2^2$ to a precision that is available for a single prime only if one is prepared to accept the use of unproven hypotheses.

In his thesis work, Schwarz also considered additive problems with more than three prime powers. For example, when $k \ge 2$, representations of the form

$$p_1^2 + p_2^4 + p_3^4 + p_4^k = n \tag{1.7}$$

or

$$p_1^2 + p_2^3 + p_3^6 + p_4^k = n \tag{1.8}$$

are considered. We focus our attention temporarily on Eq. (1.8), and on those integers n for which the congruences $x_1^2 + x_2^3 + x_3^6 + x_4^k \equiv n \bmod q$ have a solution with $(x_1x_2x_3x_4, q) = 1$, for all $q \in \mathbb{N}$. Let $\mathscr{F}_k$ denote the set of all such n. Then Schwarz shows [15, Satz 6] that when $n \le N$ and $n \in \mathscr{F}_k$ but n has no representation in the form (1.8), with all p_j prime, then n is in a set with no more than $O(N(\log N)^{-A})$ members, again for any fixed $A > 0$. There is also a corresponding result for Eq. (1.7) [15, Satz 5]. Our methods apply to such problems as well, leading to analogues of Theorems 1.1 and 1.2 with little difficulty, the overall details being somewhat simpler thanks to the presence of a fourth summand. In fact, it is possible in the two problems (1.7) and (1.8) to establish an asymptotic formula for the number of solutions, with the exceptional set estimate still of strength comparable to the conclusion in Theorem 1.1. We content ourselves with a brief discussion of such a result for Eq. (1.8). In this context, define the counting function

$$\varrho(n) = \sum_{p_1^2+p_2^3+p_3^6+p_4^k=n} (\log p_1)(\log p_2)(\log p_3)\log p_4 \tag{1.9}$$

and the singular series

$$\mathfrak{s}(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{\substack{1\le x_j\le q\\1\le j\le 4\\(x_j,q)=1}} \varphi(q)^{-4} e(a(x_1^2 + x_2^3 + x_3^6 + x_4^k - n)/q). \tag{1.10}$$

Theorem 1.3 *Let $k \ge 2$ be a natural number, and let $A > 1$. Then the inequality*

$$\left|\varrho(n) - \Gamma(\tfrac{1}{2})\Gamma(\tfrac{4}{3})\Gamma(\tfrac{7}{6})\mathfrak{s}(n)n^{1/k}\right| > n(\log n)^{-A}$$

holds for no more than $O(N^{1-1/(8k^2)+\varepsilon})$ *of the natural numbers* n *not exceeding* N. *Further, there is a number* $C \geq 1$ *such that for* $n \in \mathscr{F}_k$ *one has*

$$\mathfrak{s}(n) \gg (\log\log n)^{-C}. \tag{1.11}$$

In particular, all but $O(N^{1-1/(8k^2)+\varepsilon})$ of the numbers $n \in \mathscr{F}_k$ with $1 \leq n \leq N$ have a representation in the form (1.8). It should be noted that $\mathscr{F}_k$ is a union of finitely many arithmetic progressions (see [15, Satz 6]), and is therefore a set of positive density.

Throughout this paper, we apply the convention that whenever the letter ε occurs in a statement, it is asserted that this statement holds for all positive real numbers ε. Constants implicit in Landau's and Vinogradov's well-known symbols may depend on ε. Eulers totient is $\varphi(n)$, and $\omega(n)$ is the number of distinct prime factors of n.

2 A Mean Value Estimate

We begin our deliberations by discussing a moment estimate for a certain Weyl sum that we now introduce. Let $k \geq 3$, and put

$$h_0(\alpha, X) = \sum_{1 \leq x \leq X} e(\alpha x^k). \tag{2.1}$$

Let $M = X^{1/k}$, and let $\mathscr{P}$ denote the set of primes p with $p \equiv -1 \bmod k$ and $M < p \leq 2M$. Then, for $t \in \mathbb{N}$, we define the sum $h_t(\alpha, X)$ by means of the recursion

$$h_t(\alpha, X) = \sum_{p \in \mathscr{P}} h_{t-1}(\alpha p^k, X/p). \tag{2.2}$$

By (2.1) and (2.2), it follows that one may also write

$$h_t(\alpha, X) = \sum_{x \leq X} w_t(x, X) e(\alpha x^k) \tag{2.3}$$

where $w_0(x, X)$ is the indicator function on $\{1, 2, \dots, [X]\}$, and where for $t \geq 1$, the coefficients $w_t(x, X)$ satisfy the relation

$$w_t(x, X) = \sum_{\substack{p \mid x \\ p \in \mathscr{P}}} w_{t-1}(x/p, X/p). \tag{2.4}$$

The sum on the right-hand side of (2.4) has at most $k-1$ summands. By induction on t, it follows that $w_t(x,X) = 0$ for $x > X$, and that for $x \le X$ one has

$$w_t(x,X) \le k^t. \tag{2.5}$$

For $t \ge 0$ and $s \ge 1$, we shall bound the mean value

$$I(X,s,t) = \int_0^1 |h_0(\alpha,X)|^2 |h_t(\alpha,X)|^{2s}\,\mathrm{d}\alpha. \tag{2.6}$$

It will be convenient to write $\theta = 1 - 1/k$.

Lemma 2.1 *For $t \ge 0$ and $s \ge 1$, one has*

$$I(X,s,t) \ll X^{2s+2-k+k(\theta^t+3\theta^s)}. \tag{2.7}$$

This estimate should be compared with Lemma 2.1 of Brüdern and Perelli [4] where a slightly superior estimate was obtained, yet with a Weyl sum that is not as flexible as our h_t. Indeed, the Weyl sum used in [4] arises through the same recursion process as our h_t, but one would start with the extra constraint in (2.1) that the x are restricted to primes. With the Riemann Hypothesis for Dirichlet L-functions in hand, this makes little difference, but in unconditional work our new Weyl sum is much easier to use. This will become transparent in Sect. 4 below.

We now commence the proof of the lemma. By (2.3) and (2.5), we have $h_t(\alpha) \ll X$, and consequently, by (2.6), one has the trivial bound $I(X,s,t) \ll X^{2s+2}$. When $t = 0$, this already established (2.7), for all s. Further, when $1 \le s \le k$, one has $\theta^s \ge \theta^k \ge 1/\mathrm{e} > 1/3$, and (2.7) is again evident.

We may now suppose that $s > k$ and $t \ge 1$, and then proceed by induction on $s+t$. By orthogonality, (2.6), (2.2) and (2.3), one finds that $I(X,s,t)$ equals the number of solutions of the diophantine equation

$$x_1^k - x_2^k = \sum_{j=1}^{2s} (-1)^j p_j^k y_j^k, \tag{2.8}$$

each solution counted with multiplicity

$$\prod_{j=1}^{2s} w_{t-1}(y_j, X/p_j), \tag{2.9}$$

and the natural numbers x_l and the primes p_j subject to $1 \le x_l \le X$ and $p_j \in \mathscr{P}$. It may be worth remarking that we have $p_j y_j \le X$ for all $1 \le j \le 2s$ whenever the multiplicity (2.9) is non-zero.

Let I_0 denote the number of solutions of (2.8), counted with weight (2.9), where for all $1 \le j \le 2s$ one has $p_j \mid x_1$ and $p_j \mid x_2$. For $l = 1$ or 2, let I_l denote the

number of solutions of (2.8) where $p_1 \nmid x_l$, counted with weight (2.9). Then, since for any solution counted by $I(X, s, t)$ but not by I_0, there is some j such that p_j does not divide one of x_1, x_2, we deduce by symmetry that

$$I(X, s, t) \le I_0 + 2s(I_1 + I_2). \tag{2.10}$$

We require an upper bound for I_0. For $\mathbf{p} = (p_1, \dots, p_{2s}) \in \mathscr{P}^{2s}$, let

$$G(\alpha, \mathbf{p}) = \sum_{\substack{1 \le x \le X \\ p_j \mid x \, (1 \le j \le 2s)}} e(\alpha x^k). \tag{2.11}$$

Then, by orthogonality and the triangle inequality, and then applying the elementary bound $|z_1 z_2 \dots z_{2s}| \ll |z_1|^{2s} + \dots + |z_{2s}|^{2s}$, we infer that

$$\begin{aligned} I_0 &\le \sum_{\mathbf{p} \in \mathscr{P}^{2s}} \int_0^1 |G(\alpha, \mathbf{p})|^2 |h_{t-1}(\alpha p_1^k, X/p_1) \dots h_{t-1}(\alpha p_{2s}^k, X/p_{2s})| \, \mathrm{d}\alpha \\ &\ll \sum_{\mathbf{p} \in \mathscr{P}^{2s}} \int_0^1 |G(\alpha, \mathbf{p})|^2 |h_{t-1}(\alpha p_1^k, X/p_1)|^{2s} \, \mathrm{d}\alpha. \end{aligned} \tag{2.12}$$

Note that at most $k-1$ different primes $p_j \in \mathscr{P}$ can divide a number x with $x \le X$. Hence, for the sum in (2.11) to be non-empty, at most $k-1$ of the entries of $\mathbf{p}$ can be distinct, and we may restrict the sum in (2.12) to such $\mathbf{p}$, of which there are no more than $O(M^{k-1})$ choices. For a fixed such choice, we deduce from orthogonality that the integral in (2.12) does not exceed the number of solutions of the diophantine equation

$$x_1^k - x_2^k = p_1^k (y_1^k - y_2^k + \dots + y_{2s-1}^k - y_{2s}^k), \tag{2.13}$$

with the variables x_1, x_2 constrained to $1 \le x_l \le X$ and $p_1 \mid x_l$ $(l = 1, 2)$, each solution counted with weight

$$\prod_{j=1}^{2s} w_{t-1}(y_j, X/p_1). \tag{2.14}$$

We put $x_l = p_1 z_l$ in (2.13) and use orthogonality again to conclude from (2.6) that

$$\int_0^1 |G(\alpha, \mathbf{p})|^2 |h_{t-1}(\alpha p_1^k, X/p_1)|^{2s} \, \mathrm{d}\alpha \le I(X/p_1, s, t-1). \tag{2.15}$$

But $p_1 \in \mathscr{P}$ so that $p_1 > M$, and then the induction hypothesis supplies the bound

$$I(X/p_1, s, t-1) \ll (X/M)^{2s+2-k+k(\theta^{t-1}+3\theta^s)}.$$

By (2.12) and (2.15), we then deduce that

$$I_0 \ll M^{k-1}(X/M)^{2s+2-k+k(\theta^{t-1}+3\theta^s)} \ll X^{\mu}$$

where

$$\begin{aligned}\mu &= \theta + \theta\big(2s+2-k+k(\theta^{t-1}+3\theta^s)\big)\\ &\le 2s+2-k+k(\theta^t+3\theta^s)+\theta-\frac{1}{k}(2s+2-k).\end{aligned}$$

Hence, since $s > k$, we see that

$$I_0 \ll X^{2s+2-k+k(\theta^t+3\theta^s)}, \tag{2.16}$$

as required.

We now proceed by considering cases. First suppose that $I_1 + I_2 \le I_0$. Then, by (2.10), we conclude that $I(X,s,t) \ll I_0$, and (2.7) follows from (2.16).

This leaves the case where $I_0 < I_1 + I_2$. Write

$$H_p(\alpha) = \sum_{\substack{1\le x\le X\\ p\nmid x}} e(\alpha x^k).$$

Then, for $l = 1$ and 2, we infer by orthogonality that

$$I_l = \sum_{p\in\mathscr{P}} \int_0^1 H_p(\alpha)h_{t-1}((-1)^{l+1}p^k\alpha, X/p)h_0(-\alpha)h_t((-1)^l\alpha)|h_t(\alpha)|^{2s-2}\,\mathrm{d}\alpha,$$

where now we write $h_t(\alpha) = h_t(\alpha, X)$ in the interest of brevity. By Hölder's inequality and (2.6), one finds that

$$I_l \le \sum_{p\in\mathscr{P}} J_p^{\frac{1}{2s}} K_p^{\frac{1}{2}-\frac{1}{2s}} I(X,s,t)^{\frac{1}{2}}, \tag{2.17}$$

where

$$J_p = \int_0^1 |H_p(\alpha)|^2 |h_{t-1}(p^k\alpha, X/p)|^{2s}\,\mathrm{d}\alpha$$

and

$$K_p = \int_0^1 |H_p(\alpha)|^2 |h_t(\alpha)|^{2s}\,\mathrm{d}\alpha.$$

Note that the right-hand side of (2.17) is independent of l. Furthermore, by orthogonality and a consideration of the underlying diophantine equations, one has $K_p \le I(X,s,t)$. In the case under consideration, (2.10) yields $I(X,s,t) \ll I_1 + I_2$, and (2.17) delivers

$$I(X,s,t)^{1/(2s)} \ll \sum_{p\in\mathscr{P}} J_p^{1/(2s)}. \tag{2.18}$$

Fix a prime $p_1 \in \mathscr{P}$. Then, by orthogonality one finds that J_{p_1} is equal to the number of solutions of Eq. (2.13) with $1 \le x_1 \le X$, $1 \le x_2 \le X$, $p_1 \nmid x_1x_2$, each solution counted with multiplicity (2.14). By (2.13), we have $x_1^k \equiv x_2^k \bmod p_1^k$, and since $p_1 \in \mathscr{P}$, it follows that $p_1^k \mid x_1 - x_2$. However, $|x_1 - x_2| < X = M^k < p_1^k$ so that we must have $x_1 = x_2$. Hence, by (2.5), (2.6) and orthogonality again, we conclude that $J_{p_1} \ll XI(X/p_1, s-1, t-1)$. Since $X/p_1 \le X^\theta$, we first deduce from the induction hypothesis and (2.7) that

$$J_{p_1} \ll X^{1+\theta(2s-k)+k(\theta^t+3\theta^s)},$$

and then infer from (2.18) the final bound

$$I(X,s,t) \ll M^{2s}X^{1+\theta(2s-k)+k(\theta^t+3\theta^s)} = X^{2s+2-k+k(\theta^t+3\theta^s)},$$

completing the induction.

3 The Basic Argument

In this section, we shall present the basic argument that underpins all proofs. Along the way, we shall establish Theorem 1.1. Let $k \ge 3$, and consider the Weyl sums

$$f(\alpha) = \sum_{\frac14 N<p^2\le N} e(\alpha p^2)\log p, \quad g(\alpha) = \sum_{\frac14 N<p^k\le N} e(\alpha p^k)\log p. \tag{3.1}$$

Whenever $\mathscr{B} \subset [0,1]$ is measurable, we put

$$r_{\mathscr{B}}(n,N) = \int_{\mathscr{B}} f(\alpha)^2 g(\alpha) e(-\alpha n)\,\mathrm{d}\alpha. \tag{3.2}$$

By orthogonality,

$$r_{[0,1]}(n,N) = \sum_{\substack{p_1^2+p_2^2+p_3^k=n\\ \frac14 N<p_1^2,p_2^2,p_3^k\le N}} (\log p_1)(\log p_2)\log p_3.$$

For $N < n \le 2N$, $n \in \mathscr{H}_k$, one expects $r_{[0,1]}(n,N)$ to be of size $N^{1/k}$, and we proceed to establish this for almost all n. Let

$$Q = N^{1/(4k)}, \tag{3.3}$$

and write $\mathfrak{M}$ for the union of the intervals

$$\{\alpha \in [0,1] : |q\alpha - a| \le QN^{-1}(\log N)^{-30k}\}$$

with $0 \le a \le q$, $(a,q) = 1$ and $1 \le q \le Q$. We also put $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.

The evaluation of $r_{\mathfrak{M}}(n,N)$ we are fortunate to be able to borrow from the work of Li [10]. Let

$$\mathfrak{S}(n,Q) = \sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{x_1,x_2,x_3=1 \\ (x_1x_2x_3,q)=1}}^{q} \varphi(q)^{-3} e(a(x_1^2 + x_2^2 + x_3^k - n)/q),$$

$$\mathfrak{J}(n,N) = \sum_{\substack{m_1+m_2+m_3=n \\ \frac{1}{4}N < m_1,m_2,m_3 \le N}} (m_1m_2)^{-1/2} m_3^{(1/k)-1}. \tag{3.4}$$

Then[2] Proposition 2.1 of Li [10] asserts that whenever $N < n \le 2N$, one has

$$r_{\mathfrak{M}}(n,N) = \frac{1}{4k}\mathfrak{S}(n,Q)\mathfrak{J}(n,N) + O(N^{1/k}(\log N)^{-30k}),$$

and for these n, the lower bound $\mathfrak{J}(n,N) \gg N^{1/k}$ is immediate. Further, Lemma 3.1 of Li [10] yields $\mathfrak{S}(n,Q) \gg (\log N)^{-15k}$ for all but $O(N^{1-1/(8k)+\varepsilon})$ of the integers $n \in \mathscr{H}_k$ with $N < n \le 2N$. This establishes the following result:

Lemma 3.1 *For all but $O(N^{1-1/(9k)})$ of the integers $n \in \mathscr{H}_k$ with $N < n \le 2N$, one has $r_{\mathfrak{M}}(n,N) \gg N^{1/k}(\log N)^{-15k}$.*

Our treatment of the minor arcs depends on an important estimate of Kumchev [8] that we now describe in a language suitable for application within this paper. Let $1 \le Y \le N^{1/8}$, and let $\mathfrak{N}(Y)$ denote the union of the pairwise disjoint intervals

$$\mathfrak{N}_{q,a}(Y) = \{\alpha \in [0,1] : |q\alpha - a| \le Y/N\}$$

with $0 \le a \le q$, $(a,q) = 1$ and $1 \le q \le Y$. We write $\mathfrak{N} = \mathfrak{N}(N^{1/8})$ and $\mathfrak{n} = [0,1] \setminus \mathfrak{N}$. We define the function $\Upsilon : [0,1] \to [0,1]$ by putting $\Upsilon(\alpha) = 0$ for $\alpha \in \mathfrak{n}$,

[2] An oversight in [10] is corrected here. The variables p_1^2, p_2^2, p_3^k run over $(\frac{1}{2}N, N]$ in [10], but then $\mathfrak{J}(n,N) = 0$ for $n < \frac{3}{2}N$ which is not acceptable. If these variables run over $(\frac{1}{4}N, N]$ instead, as we have arranged matters here, then the proof of Proposition 2.1 in Li [10] becomes valid.

and when $\alpha \in \mathfrak{N} \cap \mathfrak{N}_{q,a}(N^{1/8})$ by writing

$$\Upsilon(\alpha) = (q + N|q\alpha - a|)^{-1}.$$

Lemma 3.2 *Uniformly for* $\alpha \in [0, 1]$, *one has*

$$|f(\alpha)|^2 \ll N^{7/8+\varepsilon} + N^{1+\varepsilon}\Upsilon(\alpha).$$

Proof Theorem 3 of Kumchev [8] provides an estimate slightly stronger than that claimed in Lemma 3.2, but for the sum

$$\sum_{\frac{1}{4}N<p^2\le N} e(\alpha p^2).$$

Thus, Lemma 3.2 follows by partial summation.

Before embarking on the estimation of the minor arc integral, we collect a number of mean value estimates. The first of these is the inequality

$$\int_0^1 |f(\alpha)|^4 \,\mathrm{d}\alpha \ll N^{1+\varepsilon} \tag{3.5}$$

that follows from a consideration of the underlying diophantine equation and Hua's lemma [18, Lemma 2.5]. Further, when $k = 3$, we put $u = 4$, and when $k \ge 4$, we put $u = k^2$. Then, the upper bound

$$\int_0^1 |g(\alpha)|^{2u} \,\mathrm{d}\alpha \ll N^{(2u/k)-1+\varepsilon} \tag{3.6}$$

is again a consequence of Hua's lemma in the special case $k = 3$, and for larger k this bound follows from Wooley's estimates for Vinogradov's mean value (for example, [20, Corollary 1.2], where an even stronger bound is obtained) and a consideration of the underlying diophantine equation.

We initiate the minor arc analysis by applying Bessel's inequality to (3.2). Thus

$$\sum_{N<n\le 2N} r_{\mathfrak{m}}(n, N)^2 \le \int_{\mathfrak{m}} |f(\alpha)|^4 |g(\alpha)|^2 \,\mathrm{d}\alpha. \tag{3.7}$$

By Hölder's inequality,

$$\int_{\mathfrak{n}} |f(\alpha)|^4 |g(\alpha)|^2 \,\mathrm{d}\alpha \le \sup_{\alpha\in\mathfrak{n}} |f(\alpha)|^{4/u} \Big(\int_0^1 |f(\alpha)|^4 \,\mathrm{d}\alpha \Big)^{1-1/u} \Big(\int_0^1 |g(\alpha)|^{2u} \,\mathrm{d}\alpha \Big)^{1/u}.$$

Hence, by (3.5), (3.6) and Lemma 3.2,

$$\int_{\mathfrak{n}} |f(\alpha)|^4 |g(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{7/(4u)+\varepsilon} N^{1-1/u} N^{(2/k)-1/u} \ll N^{1+(2/k)-\delta+\varepsilon}, \tag{3.8}$$

where $\delta = 1/(4u)$.

This leaves the set $\mathfrak{N} \cap \mathfrak{m}$ for treatment, and this set is covered by the union of sets $\mathfrak{K}(Y) = \mathfrak{N}(2Y) \setminus \mathfrak{N}(Y)$ as Y runs over $2^{-j}N^{1/8}$, with $Q(\log N)^{-30k} \le Y \le \frac{1}{2}N^{1/8}$. Note that $\Upsilon(\alpha) \le Y^{-1}$ for $\alpha \notin \mathfrak{N}(Y)$. Further, Lemma 2 of Brüdern [2] supplies the bound

$$\int_{\mathfrak{N}(2Y)} \Upsilon(\alpha) |g(\alpha)|^2 \,\mathrm{d}\alpha \ll YN^{1/k+\varepsilon-1} + N^{2/k+\varepsilon-1}.$$

This implies that

$$\int_{\mathfrak{K}(Y)} \Upsilon(\alpha)^2 |g(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{1/k+\varepsilon-1} + Y^{-1}N^{2/k+\varepsilon-1}.$$

For $\alpha \in \mathfrak{N}$, we deduce from Lemma 3.2 that $|f(\alpha)|^2 \ll N^{1+\varepsilon}\Upsilon(\alpha)$. Hence, on summing over Y, we infer that

$$\int_{\mathfrak{N}\cap\mathfrak{m}} |f(\alpha)|^4 |g(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{1+7/(4k)+\varepsilon}. \tag{3.9}$$

Note that this bound is superior to the one in (3.8), so that we now deduce from (3.7) that

$$\sum_{N<n\le 2N} r_{\mathfrak{m}}(n,N)^2 \ll N^{1+2/k-\delta+\varepsilon}.$$

Consequently, the inequality $|r_{\mathfrak{m}}(n,N)| > N^{1/k}(\log N)^{-30k}$ can hold for no more than $O(N^{1-\delta+\varepsilon})$ of the integers $n \in (N, 2N]$. The conclusion of Theorem 1.1 now follows by combining this last observation with Lemma 3.1 and a dyadic splitting up argument.

4 A Variant of the Main Theme

We now tune the basic argument to deliver Theorem 1.2. Fix $k \ge 4$, and recall that $\theta = 1 - 1/k$. Then choose $t \in \mathbb{N}$ such that $\theta^{t-1} > \frac{1}{36} \ge \theta^t$. With this choice of t, we put $h(\alpha) = h_t(\alpha, N^{1/k})$. With $f(\alpha)$ as in (3.1), we define

$$r^*_{\mathscr{B}}(n,N) = \int_{\mathscr{B}} f(\alpha)^2 h(\alpha) e(-\alpha n) \,\mathrm{d}\alpha,$$

where $\mathscr{B} \subset [0,1]$ denotes a measurable set. By orthogonality, (3.1) and (2.3), one has

$$r^*_{[0,1]}(n,N) = \sum_{\substack{p_1^2+p_2^2+x^k=n \\ \frac{1}{4}N<p_1^2,p_2^2\le N}} w_t(x;N^{1/k})(\log p_1)\log p_2. \tag{4.1}$$

Much as in the previous section, we expect that for most $n \in (N,2N] \cap \mathscr{G}_k$ the count $r^*_{[0,1]}(n,N)$ comes close to $n^{1/k}$, and this can be established by invoking Lemma 2.1 in place of (3.6) within the minor arc work performed in the previous section. However, the use of the sums $h(\alpha)$ causes extra complication in the major arc analysis.

We overwrite previous usage by now putting

$$Q = N^{\theta^t/k}.$$

Let $\mathfrak{M}$ and $\mathfrak{m}$ be defined as in Sect. 3, but with this new value of Q. The arcs $\mathfrak{N}$, $\mathfrak{N}(X)$ and $\mathfrak{n}$ retain their meaning from Sect. 3. We now mimic the argument departing from (3.7). Put $s = 4k$ and then apply Hölder's inequality to see that

$$\int_{\mathfrak{n}} |f(\alpha)|^4|g(\alpha)|^2\,\mathrm{d}\alpha \le \sup_{\alpha\in\mathfrak{n}}|f(\alpha)|^{4/s}\Big(\int_0^1 |f(\alpha)|^4\,\mathrm{d}\alpha\Big)^{1-1/s}\Big(\int_0^1 |h(\alpha)|^{2s}\,\mathrm{d}\alpha\Big)^{1/s}.$$

By Lemma 2.1, (3.5) and Lemma 3.2, we discern that

$$\int_{\mathfrak{n}} |f(\alpha)^4h(\alpha)^2|\,\mathrm{d}\alpha \ll N^{7/(4s)+\varepsilon}N^{1-1/s}(N^{(2s/k)-1+\theta^t+3\theta^s})^{1/s} \ll N^{1+(2/k)+\lambda+\varepsilon}, \tag{4.2}$$

where

$$\lambda = \frac{1}{s}\Big(\theta^t + 3\theta^s - \frac{1}{4}\Big).$$

Recall the definition of t, and observe that $\theta^k \le \mathrm{e}^{-1}$ and $\mathrm{e}^4 > 54$. It is now readily confirmed that

$$\lambda \le \frac{1}{s}\Big(3\theta^s - \frac{2}{9}\Big) \le -\frac{1}{24k}. \tag{4.3}$$

Next, we consider the range $\mathfrak{N} \cap \mathfrak{m}$. Mimicry of the deduction of (3.9) yields

$$\int_{\mathfrak{N}\cap\mathfrak{m}} |f(\alpha)|^4|h(\alpha)|^2\,\mathrm{d}\alpha \ll N^{1+2/k+\varepsilon}Q^{-1}.$$

Now, since $k \ge 4$ and $\theta^t \ge \frac{1}{36}\theta > \frac{1}{48}$, we infer from (4.2) and (4.3) that

$$\int_{\mathfrak{m}} |f(\alpha)|^4 |h(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{1+\frac{2}{k}-\frac{1}{48k}}.$$

By using Bessel's inequality as in (3.7), this estimate allows us to conclude as follows:

Lemma 4.1 *For all but $O(N^{1-1/(49k)})$ of the integers $n \in (N, 2N]$ one has $|r^*_{\mathfrak{m}}(n, N)| < N^{1/k}(\log N)^{-100k}$.*

For the major arcs, we have to prepare for an application of the methods of Liu and Zhan [11] with quite some effort. We begin with an explicit formula for the sums $h(\alpha)$. Put $P = N^{1/k}$. With t still as above, let $\mathscr{U}(N)$ denote the set of all tuples $\mathbf{p} = (p_1, \dots, p_t)$ built from primes $p_j \equiv -1 \bmod k$ $(1 \le j \le t)$ that satisfy the inequalities

$$P^{1/k} < p_1 \le 2P^{1/k}, \quad (P/(p_1 \dots p_j))^{1/k} < p_{j+1} \le 2(P/(p_1 \dots p_j))^{1/k} \quad (1 \le j < t). \tag{4.4}$$

For $\mathbf{p} \in \mathscr{U}(N)$ we write $u = u(\mathbf{p}) = p_1 p_2 \dots p_t$. Then, repeated use of (2.2) yields

$$h(\alpha) = \sum_{\mathbf{p} \in \mathscr{U}(N)} \sum_{x \le P/u} e(\alpha(ux)^k). \tag{4.5}$$

We summarize some estimates concerning $\mathscr{U}(N)$ in the next lemma.

Lemma 4.2 *For all $\mathbf{p} \in \mathscr{U}(N)$ one has $u(\mathbf{p}) \asymp P^{1-\theta^t}$. Further,*

$$\#\mathscr{U}(N) \asymp P^{1-\theta^t}(\log N)^{-t}.$$

Proof An inspection of (4.4) shows that there exist constants $0 < c'_{1,j} < c_{1,j} < c_{2,j} < c'_{2,j}$ with the property that whenever $c_{1,j}P^{\theta^{j-1}} < p_j < c_{2,j}P^{\theta^{j-1}}$ holds for all $1 \le j \le t$, then $\mathbf{p} \in \mathscr{U}(N)$, and whenever $\mathbf{p} \in \mathscr{U}(N)$, then $c'_{1,j}P^{\theta^{j-1}} < p_j < c'_{2,j}P^{\theta^{j-1}}$ for all j. The conclusions of Lemma 4.2 now follow from Chebychev's estimates.

We are ready to develop a major arc approximation for the sum $h(\alpha)$. When $a \in \mathbb{Z}$, $q \in \mathbb{N}$ and $\beta \in \mathbb{R}$, we put

$$S(q, a) = \sum_{x=1}^{q} e(ax^k/q), \quad V(\beta, Y) = \int_0^Y e(\beta\gamma^k)\,\mathrm{d}\gamma.$$

Then, according to Theorem 4.1 of Vaughan [18], one has

$$\sum_{x \le P/u} e\Big(\Big(\frac{a}{q} + \beta\Big)(ux)^k\Big) = q^{-1}S(q, au^k)V(\beta u^k, P/u) + O(q^{\varepsilon}(q + Nq|\beta|)^{1/2}).$$

A change of variable shows that $V(\beta u^k, P/u) = u^{-1}V(\beta, P)$. Hence, on taking $\alpha = (a/q) + \beta$ in (4.5), we deduce from Lemma 4.2 that

$$h(\alpha) = V(\beta, P) \sum_{\mathbf{p} \in \mathscr{U}(N)} \frac{S(q, au^k)}{qu} + O\big(P^{1-\theta'} q^{\varepsilon} (q + Nq|\beta|)^{1/2}\big)\big)$$

where again we wrote $u = u(\mathbf{p})$ in the interest of brevity. Next, consider the sum

$$v(\beta) = \frac{1}{k} \sum_{m \le N} m^{-\theta} e(\beta m).$$

Maclaurin's summation formula yields $V(\beta, P) = v(\beta) + O(1 + P|\beta|)$. Hence, if we define the function $h^*(\alpha)$ for $\alpha = (a/q) + \beta \in \mathfrak{M}$ with $q \le Q$, $(a, q) = 1$ and $|\beta| \le Q/N$ by

$$h^*(\alpha) = v(\beta) \sum_{\mathbf{p} \in \mathscr{U}(N)} \frac{S(q, au^k)}{qu}, \tag{4.6}$$

we find that uniformly for $\alpha \in \mathfrak{M}$ one has

$$h(\alpha) = h^*(\alpha) + O(P^{1-\frac{1}{2}\theta'+\varepsilon}).$$

Let

$$r'(n, N) = \int_{\mathfrak{M}} h^*(\alpha) f(\alpha)^2 e(-\alpha n)\, \mathrm{d}\alpha.$$

Then, via Bessel's inequality, we deduce from the previous estimate that

$$\sum_{N < n \le 2N} \big(r^*_{\mathfrak{M}}(n, N) - r'(n, N)\big)^2 \le \int_{\mathfrak{M}} |(h(\alpha) - h^*(\alpha)) f(\alpha)^2|^2\, \mathrm{d}\alpha \ll P^{2-\theta'+\varepsilon} N,$$

and we may conclude as follows:

Lemma 4.3 *For all but $O(N^{1-1/(49k)})$ of the integers $n \in (N, 2N]$ one has*

$$|r^*_{\mathfrak{M}}(n, N) - r'(n, N)| < N^{1/k} (\log N)^{-100k}.$$

We now evaluate $r'(n, N)$ further, replacing the exponential sum $f(\alpha)$ by its natural approximation. This is straightforward by the method proposed in [11]. In this process we receive help from the function $h^*(\alpha)$, as this decays in q. To see this, note that whenever $(a, q) = 1$, one finds from Theorem 4.2 of Vaughan [18]

that $q^{-1}S(q,au^k) \ll q^{-1/k}(q,u^k)^{1/k}$. Consequently, by (4.6), Lemma 4.2 and [18, Lemma 2.8],

$$h^*(\alpha) \ll P(q+P^k|q\alpha-a|)^{-1/k} \sum_{\mathbf{p}\in\mathscr{U}(N)} \frac{(q,u)}{u} \ll P(\log N)^{-t}(q+P^k|q\alpha-a|)^{-1/k}.$$

In such a situation, the method of Liu and Zhan [11] is particularly easy to apply, and on following the recent exposition of Hoffman and Yu [6], for example, one identifies a leading term, featuring the singular integral (3.4) and a kind of singular series that we now introduce. Let

$$S^*(q,a) = \sum_{\substack{x=1\\(x,q)=1}}^{q} e(ax^2/q),$$

and then put

$$A_u(q,n) = \varphi(q)^{-2}q^{-1} \sum_{\substack{a=1\\(a,q)=1}}^{q} S^*(q,a)^2 S(q,au^k)e(-an/q) \tag{4.7}$$

to form the sum

$$\Theta(n,N) = \sum_{\mathbf{p}\in\mathscr{U}(N)} u(\mathbf{p})^{-1} \sum_{q\le Q} A_{u(\mathbf{p})}(q,n). \tag{4.8}$$

Equipped with this notation, we summarize the outcome of the Liu–Zhan method in the next lemma, but as we pointed out already, there is no need to present a detailed proof because the reader will have no difficulty in providing one along the lines of Hoffmann and Yu [6, Sect. 6].

Lemma 4.4 *Let $A > 1$. Then, for all $N < n \le 2N$, one has*

$$r'(n,N) = \Theta(n,N)\mathfrak{J}(n,N) + O(N^{1/k}(\log N)^{-A}).$$

Our next task is to disentangle the sum over $\mathbf{p}$ in (4.8), and realize the partial singular series

$$\mathfrak{S}^*(n,q) = \sum_{q\le Q} A_1(q,n) \tag{4.9}$$

as a factor. With this end in view, we examine $A_u(q,n)$ more closely. The number of incongruent solutions x_1,x_2,x_3 of the congruence $x_1^2+x_2^2+(ux_3)^k \equiv n \bmod q$ with $(x_1x_2,q)=1$ is a multiplicative function of q, and by orthogonality, this function is

given by

$$q^{-1}\sum_{a=1}^{q} S^*(q,a)^2 S(q,au^k)e(-an/q).$$

Hence, by Möbius's inversion formula, we read off from (4.7) that $A_u(q,n)$ is also multiplicative as a function of q. Thus, we may restrict attention to the case where $q = p^l$ is a power of a prime. In this instance, we apply a result of Hua [7], showing that $S^*(p^l,a) = 0$ holds whenever $p \nmid a$ and $l \geq 2$ when p is odd, and also for $p = 2$, $l \geq 4$. Hence, by (4.7), for all $u \in \mathbb{N}$ one has

$$A_u(p^l,n) = 0 \quad (l \geq 2, p \geq 3, \text{ or } l \geq 4, p = 2). \tag{4.10}$$

Now suppose that p is an odd prime. When $p \mid u$, we find from (4.7) that

$$A_u(p,n) = A_p(p,n) = (p-1)^{-2}\sum_{a=1}^{p-1} S^*(p,a)^2 e(-an/p).$$

We write

$$\tau_p = \sum_{x=1}^{p} e(x^2/p), \quad c_p(n) = \sum_{a=1}^{p-1} e(-an/p).$$

Then, by familiar properties of the quadratic Gauß sum, whenever $p \nmid a$ we have

$$S^*(p,a) = \sum_{x=1}^{p} e(ax^2/p) - 1 = \Big(\frac{a}{p}\Big)\tau_p - 1.$$

Hence

$$S^*(p,a)^2 = \tau_p^2 + 1 - 2\Big(\frac{a}{p}\Big)\tau_p. \tag{4.11}$$

and

$$A_p(p,n) = (p-1)^{-2}(\tau_p^2+1)c_p(n) - 2(p-1)^{-2}\tau_p \sum_{a=1}^{p-1}\Big(\frac{a}{p}\Big)e\Big(-\frac{an}{p}\Big).$$

The remaining sum on the right transforms into $(n \mid p)_L \bar{\tau}_p$, so that

$$A_p(p,n) = (p-1)^{-2}(\tau_p^2+1)c_p(n) - 2(p-1)^{-2}|\tau_p|^2\Big(\frac{n}{p}\Big).$$

From the classical identity $|\tau_p|^2 = p$ we now conclude that

$$|A_p(p,n)| \le 8p^{-1}(p,n). \tag{4.12}$$

Next consider odd primes p with $p \nmid u$. Then, a simple transformation shows that $S(p,au^k) = S(p,a)$, and hence that $A_u(p,n) = A_1(p,n)$. When $p \nmid a$ one also has (Vaughan [18, Lemma 4.3])

$$S(p,a) = \sum_{\chi} \bar\chi(a)\tau(\chi)$$

where χ runs over the $(k,p-1)-1$ non-principal characters χ, mod p, for which χ^k is principal, and where

$$\tau(\chi) = \sum_{a=1}^{p} \chi(a)e(a/p).$$

By (4.11),

$$\begin{aligned} A_1(p,n) &= (p-1)^{-2}p^{-1} \sum_{a=1}^{p-1} \sum_{\chi} \bar\chi(a)\tau(\chi)\Big(\tau_p^2 + 1 - 2\Big(\frac{a}{p}\Big)\tau_p\Big)e\Big(-\frac{an}{p}\Big) \\ &= (p-1)^{-2}p^{-1} \sum_{\chi} \tau(\chi)(\tau_p^2+1) \sum_{a=1}^{p-1} \bar\chi(a)e\Big(-\frac{an}{p}\Big) \\ &\quad - 2(p-1)^{-2}p^{-1} \sum_{\chi} \tau(\chi)\tau_p \sum_{a=1}^{p-1} \bar\chi(a)\Big(\frac{a}{p}\Big)e\Big(-\frac{an}{p}\Big). \end{aligned}$$

When $p \mid n$, the first summand on the right vanishes, and so does the second unless $\chi = \bar\chi$ is the Legendre symbol. From the standard upper bound for Gauß sums, it now follows that $|A_1(p,n)| \le 2/(p-1)$ whenever $p \mid n$. If $p \nmid n$, then the sum over a in the first summand on the right-hand side of the preceding display again transforms into a Gauß sum, and so does the sum over a in the second summand unless again χ is the Legendre symbol, in which case the relevant sum becomes the Ramanujan sum $c_p(n)$. A short calculation now shows that whenever $p \nmid n$ one has

$$|A_1(p,n)| \le \frac{4k}{p-1} \le \frac{6k}{p}, \tag{4.13}$$

and we then see that this bound holds for all odd primes p.

Based on (4.12) and (4.13), we may now evaluate $\Theta(n,N)$ in terms of the singular series.

Lemma 4.5 *We have*

$$\Theta(n,N) = \mathfrak{S}^*(n,Q) \sum_{\mathbf{p}\in\mathscr{U}(N)} u(\mathbf{p})^{-1} + O(N^{-\theta'/k}).$$

Proof By (4.8) and (4.9),

$$\Theta(n,N) - \mathfrak{S}^*(n,Q) \sum_{\mathbf{p}\in\mathscr{U}(N)} \frac{1}{u} = \sum_{\mathbf{p}\in\mathscr{U}(N)} \frac{1}{u} \sum_{q\le Q} \big(A_u(q,n) - A_1(q,n)\big). \tag{4.14}$$

By (4.10), we may restrict the sum over q to the set

$$\mathscr{Q} = \{q \le Q : 16 \nmid q,\ p^2 \nmid q \text{ for all odd } p\}.$$

Further, for each pair $\mathbf{p}, q$ with $\mathbf{p} \in \mathscr{U}(N)$, $q \in \mathscr{Q}$ and $(u(\mathbf{p}), q) = 1$, one has $A_u(q,n) = A_1(q,n)$, so that these pairs do not contribute to (4.14). Hence the sum in (4.14) may be restricted further, to those pairs $\mathbf{p}, q$ where $(p_1p_2\dots p_t, q) > 1$.

Let I denote a non-empty subset of $\{1,2,\dots,y\}$, and let

$$\mathscr{K}(I) = \{(\mathbf{p},q) \in \mathscr{U}(N)\times\mathscr{Q} : p_i \mid q \text{ for } i\in I,\ p_j \nmid q \text{ for } j\notin I\}.$$

The argument from the preceding paragraph shows that any pair $\mathbf{p}, q$ that makes a non-zero contribution to the sum on the right-hand side of (4.14) is in some $\mathscr{K}(I)$. Now suppose that $(\mathbf{p},q) \in \mathscr{K}(I)$. Then, at least when N is large, the $p_1,\dots,p_t$ are all distinct, and hence, the number

$$u' = \prod_{i\in I} p_i$$

is a divisor of q with $(q/u', u(\mathbf{p})) = 1$. It follows that

$$A_u(q,n) = A_u(u',n)A_u(q/u',n) = A_{u'}(u',n)A_1(q/u',n),$$

and we infer that

$$A_u(q,n) - A_1(q,n) = \big(A_{u'}(u',n) - A_1(u',n)\big)A_1(q/u',n).$$

Consequently, the contribution from $(\mathbf{p},q) \in \mathscr{K}(I)$ to the sum in (4.14) is no larger than

$$\sum_{\mathbf{p}\in\mathscr{U}(N)} \frac{1}{u} \sum_{\substack{q\in\mathscr{Q}\\ q\equiv 0 \bmod u'}} \big|A_1(q/u',n)\big(A_{u'}(u',n) - A_1(u',n)\big)\big|.$$

We now write $v = q/u'$ and deduce from (4.12) and (4.13) that the expression in the preceding display is bounded by

$$\ll \sum_{\mathbf{p}\in\mathscr{U}(N)} \frac{1}{u}\Big(\sum_{v\le Q}\frac{(6k)^{\omega(v)}}{v}\Big)\frac{8^{\omega(u')}}{u'}(u',n) \ll (\log Q)^{6k}\sum_{\mathbf{p}\in\mathscr{U}(N)}\frac{(u',n)}{uu'}.$$

Here the sum over $\mathbf{p}$ factorizes. For $i \in I$ the corresponding factor does not exceed

$$\sum_{p_i \asymp N^{\theta^{i-1}/k}} \frac{(p_i,n)}{p_i^2} \ll N^{-\theta^{i-1}/k}, \tag{4.15}$$

while for $j \notin I$ the sum over p_j is certainly bounded. Since I is non-empty, we have at least one factor (4.15), producing the estimate $O(N^{-\theta^t/k})$ for the portion of (4.14) where $(\mathbf{p}, q) \in \mathscr{K}(I)$. Summation over I completes the proof of Lemma 4.5.

We now need a lower bound for the singular series. Although there is no explicit reference at hand for the sum $\mathfrak{S}^*(n, Q)$, there is no difficulty in adjusting the arguments of [9, Sect. 6] to the present needs, and we obtain the following result, analogous to Lemma 3.1 of Li [10].

Lemma 4.6 *For all but $O(NQ^{\varepsilon-1/2})$ of the integers $n \in (N, 2N] \cap \mathscr{G}_k$, one has $\mathfrak{S}^*(n, Q) \gg (\log n)^{-15k}$.*

We are ready to establish Theorem 1.2. Indeed, from Lemmas 4.2, 4.5 and 4.6, we find that $\Theta(n, N) \gg (\log N)^{-15k-t}$ holds for all but $O(N^{-1/(97k)})$ of the integers $n \in (N, 2N] \cap \mathscr{G}_k$. By Lemma 4.4 and (3.4), we deduce that for these n we also have $r'(n, N) \gg N^{1/k}(\log N)^{-15k-t}$. The definition of t implies that $t \le 5k$, and hence, by Lemmas 4.1 and 4.3, we finally see that the lower bound

$$r^*_{[0,1]}(n, N) \gg N^{1/k}(\log N)^{-20k}$$

holds for all but $O(N^{-1/(97k)})$ of the integers $n \in (N, 2N] \cap \mathscr{G}_k$. By (4.1) and a dyadic dissection argument, this confirms the conclusions recorded in Theorem 1.2.

5 The Quaternary Problem

We end with a short sketch of a proof of Theorem 1.3. Since we attempt to establish an asymptotic formula, we can no longer work with localized Weyl sums but have to use their brethren

$$F_l(\alpha) = \sum_{p^l \le N} e(\alpha p^l)\log p.$$

Then, by (1.9) and orthogonality, whenever $n \le N$ one has

$$\varrho(n) = \int_0^1 F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)e(-\alpha n)\,\mathrm{d}\alpha.$$

We define major and minor arcs $\mathfrak{M}$ and $\mathfrak{m}$ as in Sect. 3, with Q defined by (3.3). When $\mathscr{B}$ is a measurable subset of $[0,1]$, we put

$$\varrho_{\mathscr{B}}(n,N) = \int_{\mathscr{B}} F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)e(-\alpha n)\,\mathrm{d}\alpha.$$

The major arc work will not detain us for long, as this is standard for the experienced worker in the area. First, one begins by applying the now standard methods of Liu and Zhan [11], and this leads to the preliminary asymptotic relation

$$\varrho_{\mathfrak{M}}(n,N) = \Gamma(\tfrac{1}{2})\Gamma(\tfrac{4}{3})\Gamma(\tfrac{7}{6})\mathfrak{s}(n,Q)n^{1/k} + O(N^{1/k}(\log N)^{-A})$$

that is valid for any fixed $A > 1$ and all $n \le N$, and in which the partial singular series is given via

$$\mathfrak{s}(n,Q) = \sum_{q \le Q} B(q,n)$$

and

$$B(q,n) = \sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{\substack{1 \le x_j \le q\\ 1 \le j \le 4\\ (x_j,q)=1}} \varphi(q)^{-4} e(a(x_1^2 + x_2^3 + x_3^6 + x_4^k - n)/q).$$

The theory of the arithmetic function $B(q,n)$ is similar to that of $A(q,n)$ in the previous section. In particular, $B(q,n)$ is again multiplicative in q, and by an argument paralleling that leading to (4.10), (4.12) and (4.13), one finds that $B(p,n) \ll p^{-3/2}(p,n)^{1/2}$ while $B(p^l,n) = 0$ holds for all p, all $l \ge 2$. It follows easily that the sum (1.10) converges absolutely, and that $\mathfrak{s}(n) - \mathfrak{s}(n,Q) \ll n^{\varepsilon}Q^{\varepsilon-1/2}$. In particular, we see that

$$\varrho_{\mathfrak{M}}(n,N) = \Gamma(\tfrac{1}{2})\Gamma(\tfrac{4}{3})\Gamma(\tfrac{7}{6})\mathfrak{s}(n)n^{1/k} + O(N^{1/k}(\log N)^{-A}). \tag{5.1}$$

To obtain a lower bound for $\mathfrak{s}(n)$, we use multiplicativity to write the series as an Euler product which takes the shape

$$\mathfrak{s}(n) = \prod_p (1 + B(p,n)).$$

By orthogonality, one deduces that $1+B(p,n) = p(p-1)^{-4}M(p,n)$ where $M(p,n)$ is the number of incongruent solutions of the congruence $y_1^2+y_2^3+y_3^6+y_4^k \equiv n \bmod p$ with $p \nmid y_1y_2y_3y_4$. The congruence condition in Theorem 1.3 assures that $M(p,n) \geq 1$, and so the Euler factors of $\mathfrak{s}(n)$ are positive, and bounded below uniformly in n by $p(p-1)^{-4}$. Further, for $p \nmid n$, we noted earlier that $B(p,n) \ll p^{-3/2}$. Hence, we conclude that

$$\mathfrak{s}(n) \gg \prod_{p|n}(1 + B(p,n)).$$

For $p \mid n$, we mentioned already that there is a number $c > 0$ with $|B(p,n)| \leq cp^{-1}$. We apply this bound for $p \mid n$ with $p > 2c$, and use the uniform lower bound for $1 + B(p,n)$ for the smaller primes to confirm (1.11).

This leaves the minor arcs $\mathfrak{m}$. The main difficulty here is that Kumchev's exponential sum estimates refer to localized sums. We have to turn these into bounds for $F_l(\alpha)$, and this requires some care.

Lemma 5.1 *Uniformly for $\alpha \in [0,1]$, one has*

$$F_2(\alpha)^2 \ll N^{7/8+\varepsilon} + N^{1+\varepsilon}\Upsilon(\alpha), \quad F_3(\alpha)^2 \ll N^{13/21+\varepsilon} + N^{2/3+\varepsilon}\Upsilon(\alpha).$$

Proof Let $P = N^{1/2}$ and $\alpha \in [0,1]$. For $1 \leq R \leq P$, put

$$f(\alpha, R) = \sum_{R<p\leq 2R} e(\alpha p^2)\log p.$$

A dyadic dissection argument provides some $R = R(\alpha)$ with $P^{7/8} \leq R \leq \frac{1}{2}P$ and the property that

$$F_2(\alpha) = \sum_{P^{7/8}<p\leq P} e(\alpha p^2)\log p + O(P^{7/8}) \ll P^{7/8} + |f(\alpha,R)|\log N. \tag{5.2}$$

Fix a (small) $\delta > 0$. If $|f(\alpha,R)| \leq P^{7/8+\delta}$, then $F_2(\alpha) \ll P^{7/8+\delta}$. In the opposite case, we apply Dirichlet's theorem on diophantine approximation to find $a \in \mathbb{Z}$, $q \in \mathbb{N}$ with $1 \leq q \leq R^{3/2}$ and $|q\alpha - a| \leq R^{-3/2}$ before using Theorem 3 of Kumchev [8] in conjunction with partial summation. This yields

$$P^{7/8+\delta} < |f(\alpha,R)| \ll R^{7/8+\varepsilon} + R^{1+\varepsilon}(q + R^2|q\alpha - a|)^{-1/2}. \tag{5.3}$$

It follows that $q + R^2|q\alpha - a| \ll R^{2+\varepsilon}P^{-7/4-2\delta}$. For large N, this implies that $q \leq P^{1/4}$ and $|q\alpha - a| \leq P^{-7/4}$, and hence that $\alpha \in \mathfrak{N}$. The trivial bound

$$R^2(q + P^2|q\alpha - a|) \leq P^2(q + R^2|q\alpha - a|)$$

now suffices to conclude from (5.3) that $|f(\alpha,R)|^2 \ll N^{1+\varepsilon}\Upsilon(\alpha)$, and (5.2) then delivers $|F_2(\alpha)|^2 \ll N^{1+\varepsilon}\Upsilon(\alpha)$. We have now shown that whenever $\delta > 0$, one has

$$|F_2(\alpha)|^2 \ll N^{7/8+\delta} + N^{1+\varepsilon}\Upsilon(\alpha).$$

This establishes Lemma 5.1 for F_2, and the bound for F_3 follows by the same argument.

We are ready to run the basic argument from Sect. 3 for the minor arcs. One observes that

$$\int_0^1 |F_2(\alpha)F_3(\alpha)F_6(\alpha)|^2\,\mathrm{d}\alpha \ll N^{1+\varepsilon} \tag{5.4}$$

(see Schwarz [15], Lemma 1.2 and Korollar), and as in (3.6) we also have

$$\int_0^1 |F_k(\alpha)|^{2k^2}\,\mathrm{d}\alpha \ll N^{2k-1+\varepsilon}. \tag{5.5}$$

By Hölder's inequality, we find that the integral

$$\int_{\mathfrak{n}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)|^2\,\mathrm{d}\alpha$$

does not exceed

$$\sup_{\alpha\in\mathfrak{n}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)|^{2/k^2}\Big(\int_0^1 |F_2F_3F_6|^2\,\mathrm{d}\alpha\Big)^{1-1/k^2}\Big(\int_0^1 |F_k|^{2k^2}\,\mathrm{d}\alpha\Big)^{1/k^2}.$$

We now use (5.4), (5.5) and Lemma 5.1 for F_2 together with trivial bounds for F_3F_6 to conclude that

$$\int_{\mathfrak{n}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)|^2\,\mathrm{d}\alpha \ll N^{1+\frac{2}{k}+\frac{1}{8k^2}+\varepsilon}. \tag{5.6}$$

For the set $\mathfrak{N}\cap\mathfrak{m}$ the argument from Sect. 3 requires an upgrade. First we apply Lemma 2 of Brüdern [2] to confirm that

$$\int_{\mathfrak{N}} \Upsilon(\alpha)|F_6(\alpha)|^2\,\mathrm{d}\alpha \ll N^{\varepsilon-2/3},$$

and we then see via Lemma 5.1 that

$$\int_{\mathfrak{N}} |F_2(\alpha)F_6(\alpha)|^2\,\mathrm{d}\alpha \ll N^{1/3+\varepsilon}.$$

For $\alpha \in \mathfrak{N} \setminus \mathfrak{N}(N^{1/21})$, we find from Lemma 5.1 that $|F_3(\alpha)|^2 \ll N^{13/21+\varepsilon}$. The trivial bound for F_k is now enough to confirm the estimate

$$\int_{\mathfrak{N}\setminus\mathfrak{N}(N^{1/21}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{\frac{20}{21}+\frac{2}{k}+\varepsilon} \tag{5.7}$$

For $\alpha \in \mathfrak{N}(N^{1/21})$ Lemma 5.1 produces $|F_2(\alpha)F_3(\alpha)| \ll N^{5/3+\varepsilon}\Upsilon(\alpha)^2$, and then the argument leading to (3.9) delivers the bound

$$\int_{\mathfrak{N}(N^{1/21})\cap\mathfrak{m}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{1+\frac{7}{4k}+\varepsilon}.$$

This estimate combines with (5.6), (5.7) and Bessel's inequality to

$$\sum_{n\le N} \varrho_{\mathfrak{m}}(n,N)^2 \le \int_{\mathfrak{m}} |F_2(\alpha)F_3(\alpha)F_6(\alpha)F_k(\alpha)|^2 \,\mathrm{d}\alpha \ll N^{1+\frac{2}{k}-\frac{1}{8k^2}+\varepsilon}.$$

It follows that for all but $O(N^{1-1/(8k^2)+2\varepsilon})$ of the integers $n \le N$ one has $\varrho_{\mathfrak{m}}(n,N) \ll N^{1/k-\varepsilon}$. This combines with (5.1) to confirm the conclusions in Theorem 1.3.

References

1. J. Brüdern, Additive Diophantine inequalities with mixed powers. II. Mathematika **34**(2), 131–140 (1987)
2. J. Brüdern, A problem in additive number theory. Math. Proc. Camb. Philos. Soc. **103**(1), 27–33 (1988)
3. J. Brüdern, K. Kawada, Ternary problems in additive prime number theory, in *Analytic Number Theory (Beijing/Kyoto, 1999)*. Developments in Mathematics, vol. 6 (Kluwer, Dordrecht, 2002), pp. 39–91
4. J. Brüdern, A. Perelli, The addition of primes and powers. Can. J. Math. **48**(3), 512–526 (1996)
5. G. Harman, A. Kumchev, On sums of squares of primes II. J. Number Theory **130**(9), 1969–2002 (2010)
6. J.W. Hoffman, G. Yu, A ternary additive problem. Monatsh. Math. **172**(3–4), 293–321 (2013)
7. L.K. Hua, Some results in the additive prime number theory. Q. J. Math. **9**, 68–80 (1938)
8. A. Kumchev, On Weyl sums over primes and almost primes. Mich. Math. J. **54**(2), 243–268 (2006)
9. M.-C. Leung, M.C. Liu, On generalized quadratic equations in three prime variables. Monatsh. Math. **115**(1–2), 133–167 (1993)
10. T. Li, On sums of squares of primes and a kth power of prime. Rocky Mt. J. Math. **42**(1), 201–222 (2012)
11. J. Liu, T. Zhan, Sums of five almost equal prime squares. II. Sci. China Ser. A **41**(7), 710–722 (1998)
12. G.S. Lü, Note on a result of Hua. Adv. Math. **35**(3), 343–349 (2006)
13. H.L. Montgomery, R.C. Vaughan, The exceptional set in Goldbach's problem. Acta Arith. **27**, 353–370 (1975)

14. W. Schwarz, Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. I. J. Reine Angew. Math. **205**, 21–47 (1960/1961)
15. W. Schwarz, Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. II. J. Reine Angew. Math. **206**, 78–112 (1961)
16. W. Schwarz, Über die Lösbarkeit gewisser Ungleichungen durch Primzahlen. J. Reine Angew. Math. **212**, 150–157 (1963)
17. W. Schwarz, Survey on analogues of the Waring problem: diophantine inequalities, in *Conference on Additive Number Theory (Bordeaux, 1977)* (Univ. Bordeaux I, Talence, 1978), pp. 121–147
18. R.C. Vaughan, *The Hardy-Littlewood Method*. Cambridge Tracts in Mathematics, vol. 125, 2nd edn. (Cambridge University Press, Cambridge, 1997)
19. T.D. Wooley, Vinogradov's mean value theorem via efficient congruencing. Ann. Math. (2) **175**(3), 1575–1627 (2012)
20. T.D. Wooley, Multigrade efficient congruencing and Vinogradov's mean value theorem. Proc. Lond. Math. Soc. (3) **111**, 519–560 (2015)

An Improvement of Liouville's Inequality

Yann Bugeaud

To the memory of Wolfgang Schwarz

Abstract The Liouville inequality gives a lower bound for the distance between two distinct algebraic numbers in terms of their heights and their degrees. We refine the classical estimate in the special case where one of the algebraic numbers is very close to one of its Galois conjugates.

Keywords Algebraic numbers • Height • Liouville's inequality

2010 Mathematics subject classification: Primary 11J04; Secondary 11J68

1 Introduction and Results

Throughout this note, the height $H(\alpha)$ of an algebraic number α (in the complex field $\mathbf{C}$ or in a p-adic field $\mathbf{Q}_p$) is the maximum of the absolute values of the coefficients of its minimal defining polynomial over $\mathbf{Z}$ (that is, the integer polynomial of lowest positive degree, with coprime coefficients and positive leading coefficient, which vanishes at α). The Liouville inequality gives a lower bound for the distance between two distinct algebraic numbers in terms of their heights and their degrees. We state below a version of it, which is a consequence of Theorems A.1 and A.3 of [1].

Theorem 1.1 *Let α and β be distinct algebraic numbers of degree n and m, respectively. Then,*

$$|\alpha - \beta| \geq 2^{1-n}\,(n+1)^{-m+1/2}\,(m+1)^{-n/2}\,H(\alpha)^{-m}\,H(\beta)^{-n}.$$

Y. Bugeaud (✉)
Université de Strasbourg, Mathématiques 7, rue René Descartes, 67084 Strasbourg, France
e-mail: bugeaud@math.unistra.fr

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_5

Recently, it was observed in [2] that, if α and β are quadratic numbers, then Theorem 1.1 can be improved when α is very close to its Galois conjugate. A precise statement is Lemma 7.1 of [2], which we reproduce below.

Lemma 1.2 *Let α and β be real quadratic numbers. Denote by α' and β' the Galois conjugates of α and β, respectively. Assume that $\alpha, \alpha', \beta, \beta'$ are distinct. Then, we have*

$$|\alpha - \beta| \geq 0.03 \cdot \max\{|\alpha - \alpha'|^{-1}, 1\} \cdot H(\alpha)^{-2} \cdot H(\beta)^{-2}.$$

The quantity $\max\{|\alpha - \alpha'|^{-1}, 1\}$ can be as large as $H(\alpha)/\sqrt{5}$ (take for α a root of the polynomial $(m^2 + m - 1)X^2 - (2m + 1)X + 1$, where $m \geq 2$ is an integer), making then a substantial improvement on Theorem 1.1. Lemma 1.2 is a key ingredient in the proof that certain transcendental continued fractions cannot be very well approximated by quadratic numbers.

The purpose of the present note is to extend Lemma 1.2 to algebraic numbers of arbitrary degree.

Theorem 1.3 *Let α and β be distinct algebraic numbers of degree $n \geq 2$ and m, respectively. Then, for any Galois conjugate α' of α, distinct from α and satisfying $|\alpha - \alpha'| \leq 1$, we have*

$$|\alpha - \beta| \geq 2^{1-n} (n+1)^{-m+1/2} (m+1)^{-n/2} \min\{H(\alpha)^{m/2}, |\alpha - \alpha'|^{-1}\} H(\alpha)^{-m} H(\beta)^{-n}.$$

Theorem 1.3 holds if $\alpha' = \beta$, but it yields a weaker estimate than Theorem A.3 of [1], which states that the distance between two distinct conjugate algebraic numbers α and α' of degree $n \geq 2$ satisfies

$$|\alpha - \alpha'| > \sqrt{3}\, (n+1)^{-(2n+1)/2} H(\alpha)^{-n+1}. \tag{1.1}$$

An inequality similar to (1.1) was proved by Mahler [6] in 1964. As we have seen after Lemma 1.2, it is sharp for $n = 2$. Schönhage [9] (see also Evertse [5]) proved that (1.1) is also sharp for $n = 3$. However, for $n \geq 4$, we do not know whether the exponent $-n + 1$ of $H(\alpha)$ in (1.1) can be replaced by a larger number. Results of [3] show that it cannot be replaced by a quantity greater than $-\frac{n}{2} - \frac{n-2}{4(n-1)}$.

Theorem 1.3 is an immediate consequence of Theorem 3.1, which is stated and proved in Sect. 3. We display below another direct consequence of Theorem 3.1, which includes Lemma 1.2 (up to the numerical constant).

Theorem 1.4 *Let α and β be distinct algebraic numbers of degree $n \geq 2$ and m, respectively. If $m \geq 2n - 2$, then, for any Galois conjugate α' of α, distinct from α, we have*

$$|\alpha - \beta| \geq 2^{-n} (n+1)^{-m+1/2} (m+1)^{-n/2} \min\{1, |\alpha - \alpha'|^{-1}\} H(\alpha)^{-m} H(\beta)^{-n}. \tag{1.2}$$

If $H(\beta) \geq H(\alpha)^{2(n-1)/n}$, then, for any Galois conjugate α' of α, distinct from α, we have

$$|\alpha - \beta| \geq 2^{1-n}\,(n+1)^{-m-n}\,(m+1)^{-n/2}\,\min\{1, |\alpha-\alpha'|^{-1}\}\,H(\alpha)^{-m}\,H(\beta)^{-n}. \tag{1.3}$$

In the sequel, p always denotes a prime number and $|\cdot|_p$ is the p-adic absolute value defined on the field $\mathbf{Q}_p$.

The p-adic analogue of (1.1) was proved in [7], without an explicit numerical constant. An explicit estimate was obtained by Pejkovic [8], who established that the p-adic distance between two distinct conjugate algebraic numbers α and α' of degree $n \geq 2$ satisfies

$$|\alpha - \alpha'|_p \geq n^{-3n/2} H(\alpha)^{-n+1}. \tag{1.4}$$

See [8] for a discussion on how sharp (1.4) can be. Evertse (private communication) recently proved that (1.4) is sharp for $n = 3$.

The p-adic analogue of Lemma 1.2 was established in [4], where it was used to show that certain p-adic numbers cannot be very well approximated by quadratic p-adic numbers.

We prove the p-adic analogue of Theorem 1.3.

Theorem 1.5 *Let p be a prime number. Let α and β be distinct algebraic numbers in $\mathbf{Q}_p$, of degree $n \geq 2$ and m, respectively. For any Galois conjugate α' of α, distinct from α and satisfying $|\alpha - \alpha'|_p \leq 1$, we have*

$$|\alpha - \beta|_p \geq (m+1)^{-n/2}(n+1)^{-m/2}\,\min\{H(\alpha)^{m/2}, |\alpha-\alpha'|_p^{-1}\}\,H(\alpha)^{-m}H(\beta)^{-n}.$$

Theorem 1.5 is an immediate consequence of Theorem 3.2, stated and proved in Sect. 3.

The proofs of Theorems 1.3 and 1.5 are not difficult. They essentially follow the classical proof of Liouville's inequality. It is our hope that Theorems 1.3 and 1.5 have further applications beside those in [2, 4].

2 Auxiliary Results

As mentioned in the introduction, the *height* of a polynomial $P(X)$ with complex coefficients

$$P(X) = a_n X^n + \ldots + a_1 X + a_0 = a_n(X-\alpha_1)\ldots(X-\alpha_n),$$

denoted by $H(P)$, is the maximum of the moduli of its coefficients. If $P(X)$ is non-zero, its *Mahler measure* is, by definition, the quantity

$$M(P) := |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\}.$$

The Mahler measure of a complex algebraic number α, denoted by $M(\alpha)$, is the Mahler measure of its minimal defining polynomial over $\mathbf{Z}$.

Lemma 2.1 *Let α be a non-zero complex algebraic number of degree n. We have the inequalities*

$$2^{-n} H(\alpha) \le M(\alpha) \le \sqrt{n+1}\, H(\alpha).$$

Proof This is an immediate consequence of Lemma A.2 of [1]. □

For the proof of Theorem 1.5, we need an auxiliary result of Morrison [7].

Lemma 2.2 *Let $P(X) = a_n X^n + \cdots + a_1 X + a_0 = a_n(X - \alpha_1)\cdots(X - \alpha_n)$ be a polynomial with coefficients in $\mathbf{Q}_p$. Then, for any non-empty set $I \subseteq \{1, \ldots, n\}$, we have*

$$|a_n|_p \cdot \prod_{i \in I} |\alpha_i|_p \le \max_{j \in \{0,1,\ldots,n\}} |a_j|_p \tag{2.1}$$

and, if $P(X)$ is in $\mathbf{Z}[X]$ and ξ is in $\mathbf{Q}_p$, then

$$|a_n|_p \cdot \prod_{i \in I} |\xi - \alpha_i|_p \le \max\{1, |\xi|_p^n\}. \tag{2.2}$$

Proof See [7, p. 341]. □

3 Proofs

Theorems 1.3 and 1.4 are direct consequences of Theorem 3.1 below.

Theorem 3.1 *Let $P(X)$ and $Q(X)$ be non-constant integer polynomials of degree n and m, respectively. Denote by α a zero of $P(X)$ of order s and by β a zero of $Q(X)$ of order t. Assuming that $P(\beta) \neq 0$, we have*

$$|P(\beta)| \ge (n+1)^{1-m/t}\, (m+1)^{-n/(2t)}\, H(P)^{1-m/t}\, H(Q)^{-n/t}$$

and, if $\alpha_2 \neq \alpha$ is a Galois conjugate of α with $|\alpha - \alpha_2| \leq 1$,

$$\begin{aligned}|\alpha-\beta| \geq 2^{1-n/s}(n+1)^{1/(2s)-m/(st)}\,(m+1)^{-n/(2st)} \\ \times H(P)^{-m/(st)}\,H(Q)^{-n/(st)} \\ \times \min\{|\alpha-\alpha_2|^{-1}, 2^{n/(2s)-1/2}\,(n+1)^{m/(2st)-1/(4s)}\,(m+1)^{n/(4st)} \\ H(P)^{m/(2st)}\,H(Q)^{n/(2st)}\}.\end{aligned} \tag{3.1}$$

The first assertion of Theorem 3.1 immediately follows from the first assertion of Theorem A.1 in [1]. The second assertion is new.

To derive Theorems 1.3 and 1.4 from Theorem 3.1, take for $P(X)$ and $Q(X)$ the minimal defining polynomials of α and β over $\mathbf{Z}$, respectively. Theorem 1.3 easily follows since $2^{(n-1)/2}\,(n+1)^{m/2-1/4}\,(m+1)^{n/4}\,H(\beta)^{n/2} \geq 1$. To prove Theorem 1.4, we need to use the upper bound

$$|\alpha-\alpha_2|^{-1} < 3^{-1/2}(n+1)^{(2n+1)/2}\,H(\alpha)^{n-1}, \tag{3.2}$$

which is a restatement of (1.1). If $m \geq 2n-2$, then

$$2^{(n-1)/2}\,(n+1)^{m/2-1/4}\,(m+1)^{n/4}\,H(\alpha)^{m/2} \geq 2^{(n-1)/2}\,(n+1)^{n-5/4}\,(2n-1)^{n/4}\,H(\alpha)^{n-1}. \tag{3.3}$$

Since the right-hand side of (3.3) exceeds $2^{-1}\,3^{-1/2}\,(n+1)^{(2n+1)/2}\,H(\alpha)^{n-1}$, inequality (1.2) follows from (3.1), (3.2) and Theorem A.1.

If $H(\beta) \geq H(\alpha)^{2(n-1)/n}$, then

$$\begin{aligned}2^{(n-1)/2}\,(n+1)^{m/2-1/4}\,(m+1)^{n/4}\,H(\alpha)^{m/2}\,H(\beta)^{n/2} &\geq H(\alpha)^{n-1} \\ &\geq (n+1)^{-(2n+1)/2}\,|\alpha-\alpha_2|^{-1},\end{aligned}$$

by (3.2). Combined with (3.1) and Theorem A.1, this gives (1.3).

Proof of Theorem 3.1 Set $P(X) = a_n(X-\alpha_1)^{s_1}\ldots(X-\alpha_p)^{s_p}$ and $Q(X) = b_m(X-\beta_1)^{t_1}\ldots(X-\beta_q)^{t_q}$, where $\alpha = \alpha_1$, $\beta = \beta_1$, $s = s_1$, $t = t_1$, $a_n \geq 1$, $b_m \geq 1$, and the α_i's (*resp.* the β_j's) are pairwise distinct. We also assume that α_2 is a Galois conjugate of α satisfying

$$|\alpha-\alpha_2| \leq 1.$$

In particular, $s = s_1 = s_2$. Denote by $Q_1(X) = b(X-\beta_1)\ldots(X-\beta_{q_1})$ the minimal polynomial of β over $\mathbf{Z}$, where $b \geq 1$. Since the resultant of $P(X)$ and $Q_1(X)$ is a non-zero integer, we get

$$1 \leq |\mathrm{Res}(P,Q_1)| = a_n b^n\,|\alpha-\beta|^{s_1}\cdot|\alpha_2-\beta|^{s_2}\ldots|\alpha_p-\beta|^{s_p}\prod_{2\leq i\leq q_1}|P(\beta_i)|,$$

and, using that $|P(\beta_i)| \le (n+1)\,H(P)(\max\{1,|\beta_i|\})^n$ for $i = 2,\dots,q_1$, we obtain

$$1 \le a_n|\alpha-\beta|^{s_1}\cdot|\alpha_2-\beta|^{s_2}\dots|\alpha_p-\beta|^{s_p}(n+1)^{q_1-1}H(P)^{q_1-1}\left(\frac{M(Q_1)}{\max\{1,|\beta|\}}\right)^n. \tag{3.4}$$

Observe that

$$|\alpha_j-\beta| \le 2\max\{1,|\alpha_j|\}\cdot\max\{1,|\beta|\}, \quad \text{for } j = 3,\dots,p.$$

Combined with (3.4), this gives

$$1 \le 2^{n-2s}a_n|\alpha-\beta|^s\cdot|\alpha_2-\beta|^s\cdot\max\{1,|\beta|\}^{-2s}\prod_{3\le j\le p}\max\{1,|\alpha_j|\}^{s_j}$$
$$(n+1)^{q_1-1}H(P)^{q_1-1}M(Q_1)^n. \tag{3.5}$$

We distinguish two cases. If $|\alpha_2-\beta| \ge 2|\alpha-\beta|$, then

$$|\alpha-\alpha_2| \ge |\alpha_2-\beta| - |\alpha-\beta| \ge \frac{|\alpha_2-\beta|}{2}$$

and, by (3.5),

$$|\alpha-\beta|^s \ge 2^{-n+s}|\alpha-\alpha_2|^{-s}M(P)^{-1}\max\{1,|\alpha|\}^s\max\{1,|\alpha_2|\}^s\max\{1,|\beta|\}^{2s}$$
$$(n+1)^{1-q_1}H(P)^{1-q_1}M(Q_1)^{-n}.$$

Since $q_1 \le m/t$, $M(Q_1) \le M(Q)^{1/t}$, $M(Q) \le \sqrt{m+1}\,H(Q)$ and $M(P) \le \sqrt{n+1}\,H(P)$, we get

$$|\alpha-\beta|^s \ge 2^{-n+s}|\alpha-\alpha_2|^{-s}\max\{1,|\alpha|\}^s\max\{1,|\alpha_2|\}^s\max\{1,|\beta|\}^{2s}$$
$$(n+1)^{-m/t+1/2}(m+1)^{-n/(2t)}H(P)^{-m/t}H(Q)^{-n/t}. \tag{3.6}$$

If $|\alpha_2-\beta| \le 2|\alpha-\beta|$, then (3.5) implies

$$1 \le 2^{n-s}a_n|\alpha-\beta|^{2s}\cdot\max\{1,|\beta|\}^{-2s}\prod_{j\ge3}\max\{1,|\alpha_j|\}^{s_j}\cdot(n+1)^{1-q_1}H(P)^{1-q_1}M(Q_1)^{-n},$$

and a similar computation gives

$$|\alpha-\beta|^{2s} \ge 2^{-n+s}\max\{1,|\alpha|\}^s\max\{1,|\alpha_2|\}^s\max\{1,|\beta|\}^{2s}$$
$$(n+1)^{-m/t+1/2}(m+1)^{-n/(2t)}H(P)^{-m/t}H(Q)^{-n/t}. \tag{3.7}$$

The combination of (3.6) and (3.7) proves the theorem. □

Theorem 1.5 is a direct consequence of Theorem 3.2 below.

Theorem 3.2 *Let p be a prime number. Let α and β be distinct algebraic numbers in $\mathbf{Q}_p$, of degree n and m, respectively. For any Galois conjugate α' of α, distinct from α, we have*

$$|\alpha-\beta|_p \geq (m+1)^{-n/2}(n+1)^{-m/2}H(\alpha)^{-m}H(\beta)^{-n} \\ \min\{|\alpha-\alpha'|_p^{-1}, (m+1)^{n/4}(n+1)^{m/4}H(\alpha)^{m/2}H(\beta)^{n/2}\}.$$

Proof of Theorem 3.2 Let $P(X)$ and $Q(X)$ denote the minimal defining polynomials of α and β over $\mathbf{Z}$. In view of (1.4), we assume that α and β are not conjugate. Consequently, the resultant $\mathrm{Res}(P,Q)$ is a non-zero integer. By using Hadamard's inequality, it follows from the expression of the resultant as the determinant of a $(m+n)\times(m+n)$ matrix that

$$|\mathrm{Res}(P,Q)| \leq (m+1)^{n/2}(n+1)^{m/2}H(P)^m H(Q)^n.$$

We deduce that

$$|\mathrm{Res}(P,Q)|_p \geq (m+1)^{-n/2}(n+1)^{-m/2}H(P)^{-m}H(Q)^{-n}.$$

Writing $P(X)=a(X-\alpha_1)\cdots(X-\alpha_n)$ and $Q(X)=b(X-\beta_1)\cdots(X-\beta_m)$ with $a\geq 1, b\geq 1, \alpha=\alpha_1, \beta=\beta_1$, this gives the inequality

$$|a|_p^m|b|_p^n \prod_{1\leq i\leq n, 1\leq j\leq m}|\alpha_i-\beta_j|_p \geq (m+1)^{-n/2}(n+1)^{-m/2}H(P)^{-m}H(Q)^{-n}.$$

Observe that, for $j=2,\ldots,m$, we have

$$|a|_p \prod_{1\leq i\leq n}|\alpha_i-\beta_j|_p = |P(\beta_j)|_p \leq \max\{1,|\beta_j|_p^n\},$$

by (2.2). Thus, we get

$$|a|_p|b|_p^n \prod_{1\leq i\leq n}|\alpha_i-\beta|_p \prod_{2\leq j\leq m}\max\{1,|\beta_j|_p^n\} \geq (m+1)^{-n/2}(n+1)^{-m/2}H(P)^{-m}H(Q)^{-n},$$

and, noticing that $|\alpha_i-\beta|_p \leq \max\{1,|\alpha_i|_p\}\max\{1,|\beta|_p\}$ for $i=3,\ldots,n$, we deduce that

$$|a|_p|\alpha-\beta|_p\cdot|\alpha_2-\beta|_p\cdot\max\{1,|\beta|_p\}^{-2}\cdot\prod_{3\leq i\leq n}\max\{1,|\alpha_i|_p\} \\ \times|b|_p^n\prod_{1\leq j\leq m}\max\{1,|\beta_j|_p^n\} \geq (m+1)^{-n/2}(n+1)^{-m/2}H(P)^{-m}H(Q)^{-n}.$$

By (2.1) and the fact that $P(X)$ and $Q(X)$ have integer coefficients, we get that

$$|\alpha-\beta|_p \cdot |\alpha_2-\beta|_p \cdot \max\{1,|\alpha|_p\}^{-1} \cdot \max\{1,|\alpha_2|_p\}^{-1} \cdot \max\{1,|\beta|_p\}^{-2} \geq (m+1)^{-n/2}(n+1)^{-m/2} H(P)^{-m} H(Q)^{-n}.$$

If $|\alpha_2-\beta|_p > |\alpha-\beta|_p$, then $|\alpha-\alpha_2|_p = |\alpha_2-\beta|_p$ and

$$|\alpha-\beta|_p \geq |\alpha-\alpha_2|_p^{-1} \max\{1,|\alpha|_p\} \cdot \max\{1,|\alpha_2|_p\} \cdot \max\{1,|\beta|_p\}^2 \times \times (m+1)^{-n/2}(n+1)^{-m/2} H(P)^{-m} H(Q)^{-n}.$$

If $|\alpha_2-\beta|_p = |\alpha-\beta|_p$, then

$$|\alpha-\beta|_p^2 \geq \max\{1,|\alpha|_p\} \cdot \max\{1,|\alpha_2|_p\} \cdot \max\{1,|\beta|_p\}^2 \times \times (m+1)^{-n/2}(n+1)^{-m/2} H(P)^{-m} H(Q)^{-n}.$$

The combination of the latter estimates yields the theorem. □

References

1. Y. Bugeaud, *Approximation by Algebraic Numbers*. Cambridge Tracts in Mathematics, vol. 160 (Cambridge University Press, Cambridge, 2004)
2. Y. Bugeaud, Continued fractions with low complexity: transcendence measures and quadratic approximation. Compos. Math. **148**, 718–750 (2012)
3. Y. Bugeaud, A. Dujella, Root separation for irreducible integer polynomials. Bull. Lond. Math. Soc. **43**, 1239–1244 (2011)
4. Y. Bugeaud, T. Pejkovic, Quadratic approximation in $\mathbf{Q}_p$. Int. J. Number Theory **11**, 193–209 (2015)
5. J.-H. Evertse, Distances between the conjugates of an algebraic number. Publ. Math. Debr. **65**, 323–340 (2004)
6. K. Mahler, An inequality for the discriminant of a polynomial. Mich. Math. J. **11**, 257–262 (1964)
7. J.F. Morrison, Approximation of p-adic numbers by algebraic numbers of bounded degree. J. Number Theory **10**, 334–350 (1978)
8. T. Pejković, Polynomial root separation and applications. PhD thesis, Université de Strasbourg and University of Zagreb, Strasbourg, 2012
9. A. Schönhage, Polynomial root separation examples. J. Symb. Comput. **41**, 1080–1090 (2006)

Guided by Schwarz' Functions: A Walk Through the Garden of Mahler's Transcendence Method

Peter Bundschuh and Keijo Väänänen

Dedicated to the Memory of Professor Wolfgang Schwarz

Abstract In this paper, transcendence results and, more generally, results on the algebraic independence of functions and their values are proved via Mahler's analytic method. Here the key point is that the functions involved satisfy certain types of functional equations as $G_d(z^d) = G_d(z) - z/(1-z)$ in the case of $G_d(z) := \sum_{h\ge 0} z^{d^h}/(1-z^{d^h})$ for $d \in \{2,3,4,\ldots\}$. In 1967, these particular functions $G_d(z)$ were arithmetically studied by W. Schwarz using Thue–Siegel–Roth's approximation method.

Keywords Algebraic independence of functions • Mahler's method

2010 Mathematics subject classification: Primary 11J91; Secondary 11B39

1 Introduction

In 1967, Schwarz [14] studied the arithmetic nature of the particular Lambert series

$$G_d(z) := \sum_{h=0}^{\infty} \frac{z^{d^h}}{1-z^{d^h}}$$

at certain rational points of the unit interval, where d is an integer parameter. Using Thue–Siegel–Roth's approximation theorem he proved: If $d \ge 3, t \ge 2$, and

P. Bundschuh (✉)
Mathematisches Institut, Universität zu Köln, Weyertal 86-90, 50931 Köln, Germany
e-mail: pb@math.uni-koeln.de

K. Väänänen
Department of Mathematical Sciences, University of Oulu, P.O. Box 3000, 90014 Oulu, Finland
e-mail: keijo.vaananen@.oulu.fi

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_6

$0 < b < t^{1-5/(2d)}$, then $G_d(b/t)$ is transcendental. Under weaker conditions on d and b, he obtained irrationality, non-quadracity, etc. Note that, e.g., the transcendence of

$$\sum_{h=0}^{\infty} \frac{1}{2^{2^h}+1} = 2 - G_2\Big(\frac{1}{2}\Big),$$

the reciprocal sum of the Fermat numbers, was not covered by the results just quoted.

Shortly later, in the first volume of the Journal of Number Theory, Mahler [9] roughly reported on earlier work of his on the transcendence of values of functions satisfying functional equations like

$$G_d(z^d) = G_d(z) - \frac{z}{1-z} \tag{1.1}$$

(see [6–8]). In this note, Mahler suggested several directions, in which his work might possibly be extended.

It is the main aim of this article to give an impression of the development, which was initiated by Schwarz' note and Mahler's reaction. To this purpose, we consider coprime[1] $A, B \in \overline{\mathbb{Q}}[z] \setminus\{0\}$ satisfying $A(0) = 0$ and put $H := \frac{A}{B}$. This rational function has coefficients in an algebraic number field (called K), and convergence radius Δ being $+\infty$ for constant B, and the smallest absolute value of all zeros of B otherwise. Clearly, the series

$$\mathcal{H}_d(z) := \sum_{h=0}^{\infty} H(z^{d^h})$$

with integer $d \geq 2$ (*to be always assumed from now on*) is in $K[[z]]$, converges in $|z| < \min(1, \Delta)$, and satisfies the functional equation

$$\mathcal{H}_d(z^d) = \mathcal{H}_d(z) - H(z) \tag{1.2}$$

"of Mahler-type." Taking $H(z) = z/(1-z)$ we get $\mathcal{H}_d = G_d$, the *Schwarz functions*, and on taking $H(z) = z$ we get $\mathcal{H}_d = F_d$, where the so-called Fredholm series $F_d(z) = \sum_{h\geq 0} z^{d^h}$ is the prototype of a Mahler function.

[1] Here and in the sequel, $\overline{\mathbb{Q}}$ denotes the field of all complex algebraic numbers.

2 Transcendence

From Mahler's transcendence criterion in [6] (see also [12, Theorem 1.2]) we deduce

Theorem 2.1 *$\mathcal{H}_d(\alpha)$ is transcendental for any $\alpha \in \overline{\mathbb{Q}}$ with $0 < |\alpha| < \min(1, \Delta)$ and $B(\alpha^{d^j}) \neq 0$ $(j = 0, 1, \ldots)$ provided that $\mathcal{H}_d(z)$ is transcendental over $K(z)$.*

Note here that something analytical in this direction is necessary: Namely, on taking $H(z) = z/(1-z^2)$ we find $\mathcal{H}_2(z) = z/(1-z)$; thus, a transcendence result of the above type cannot hold for this $\mathcal{H}_2$.

In some good-natured cases, the transcendence of $\mathcal{H}_d(z)$ follows from classical results in function theory, e.g., if $H(z) = z$. But it is important to have rather general criteria for the transcendence of Mahler-type functions. One of those reads as follows:

Theorem 2.2 ([11]) *If $f \in \mathbb{C}[[z]]$ satisfies $f(z^d) = \varphi(z, f(z))$ or $f(z) = \psi(z, f(z^d))$ for some $\varphi, \psi \in \mathbb{C}(z, w)$, then f is either rational or transcendental.*

Thus, under favorable conditions, one has only to exclude rationality. Precisely in this direction, Coons [2, Theorem 2.2] deduced quite recently the following functional transcendence criterion from Theorem 2.2:

Theorem 2.3 *If $f \in \mathbb{C}[[z]]$ satisfies $f(z^d) = f(z) - \frac{A(z)}{B(z)}$ with $A, B \in \mathbb{C}[z] \setminus \{0\}$ and $\max(\deg A, \deg B) \leq d - 1$, then f is transcendental over $\mathbb{C}(z)$.*

Note that this implies the transcendence of all Schwarz functions $G_d(z)$. Note also that, in general, the bound $d-1$ for the degrees of A, B is best possible for any d as one can see by taking

$$A(z) = \alpha z \frac{z^{d-1} - \alpha^{d-1}}{z - \alpha}, \quad B(z) = \alpha - z^d$$

with α some $(d-1)$th root of unity, where we are led to the rational function

$$\sum_{h=0}^{\infty} \frac{A}{B}(z^{d^h}) = \frac{z}{\alpha - z}$$

(see [3, Theorem 9] and [1, Lemma 2.10]) generalizing our example $\mathcal{H}_2(z)$ after Theorem 2.1.

In the rest of this section, we include a rather shortened

Proof of Theorem 2.3 W.l.o.g. we may assume A, B coprime and, moreover, $A(0) = 0, B(0) \neq 0$. By Theorem 2.2, it is enough to show $f \notin \mathbb{C}(z)$. Thus, let us assume, on the contrary, that f is rational, say $f = u/v$ with coprime $u, v \in \mathbb{C}[z] \setminus \{0\}$. Then

the functional equation can be equivalently written as

$$u(z^d)v(z)B(z) = v(z^d)\big(u(z)B(z) - v(z)A(z)\big),$$

hence, by the coprimality of $u(z^d)$, $v(z^d)$,

$$v(z^d) \mid v(z)B(z) \quad \text{and} \quad u(z^d) \cdot \frac{v(z)B(z)}{v(z^d)} = u(z)B(z) - v(z)A(z) \tag{2.1}$$

implying $(d-1)\deg v \le \deg B$.

Now, $v = \text{const}$ would imply $B \,|A$, by the equation in (2.1), hence $B = \text{const}$ since A, B are supposed to be coprime. Thus, $u(z^d) = u(z) - (v(0)/B(0))A(z)$ implying $d \deg u \le \max(\deg u, d-1)$ hence $u = \text{const}$, and then $A = 0$, a contradiction.

So the case $\deg B \le d-2$ is excluded [see after (2.1)] implying $\deg B = d-1$, and this, in turn, leads to $\deg v \le 1$, where we may immediately assume $\deg v = 1$ or $v(z) = \alpha z + \beta$ with $\alpha \ne 0$. The degree of the left-hand side of the equation in (2.1) equals $d \deg u$, whereas the degree of the right-hand side is $\le \max(d-1+\deg u, d)$, and this consideration yields $\deg u \le 1$ or $u(z) = az + b$. Therefore the functional equation from Theorem 2.3 reduces to

$$\frac{A(z)}{B(z)} = \frac{az+b}{\alpha z+\beta} - \frac{az^d+b}{\alpha z^d+\beta} = \frac{(b\alpha - a\beta)z(z^{d-1}-1)}{(\alpha z^d+\beta)(\alpha z+\beta)}$$

with $a\beta \ne b\alpha$ since $A \ne 0$, whence

$$A(z)\big(\alpha z(z^{d-1}-1) + (\alpha z+\beta)\big)(\alpha z+\beta) = (b\alpha - a\beta)z(z^{d-1}-1)B(z)$$

implying $\deg A + 1 = \deg B \;\Leftrightarrow\; \deg A = d-2$ and, moreover,

$$A(z)(\alpha z+\beta)^2 = C(z) \cdot z(z^{d-1}-1) \tag{2.2}$$

with some $C \in \mathbb{C}[z]\setminus\{0\}$ of degree 0, hence $C(z) = \text{const} \ne 0$. Thus, the right-hand side of (2.2) has only simple zeros but the left-hand side has multiple ones, and this contradiction concludes our proof. □

3 Hypertranscendence

An analytic function is called *hypertranscendental* if no finite collection of derivatives of the function is algebraically dependent over $\mathbb{C}(z)$. A hypertranscendence criterion for Mahler-type functions is the following:

Theorem 3.1 ([10, Theorem 3]) *Suppose that $f \in \mathbb{C}[[z]]$ has the following two properties:*

(i) *For some integer $n \geq 1$, let $f, f', \ldots, f^{(n-1)}$ be algebraically dependent over $\mathbb{C}(z)$.*
(ii) *For some integer $d \geq 2$, f satisfies $f(z^d) = u(z)f(z) + v(z)$, where $u, v \in \mathbb{C}(z), u \neq 0$. If $u(z) = s_M z^M + \ldots$ with an integer M and $s_M \neq 0$, put $Q = [M/(d-1)]$.*

Then there exists some $w \in \mathbb{C}(z)$ satisfying

$$w(z^d) = u(z)w(z) + v(z) \quad \text{or} \quad w(z^d) = u(z)w(z) + v(z) - \gamma \frac{u_1(z)z^{Qd}}{u_2(z)},$$

where $u_1(z) = u(z)/(s_M z^M), u_2 \in \mathbb{C}(z) \setminus \{0\}$ fulfills the condition $u_2(z^d) = u_2(z)/u_1(z)$, and $\gamma \in \mathbb{C}$ is the constant term in the z-expansion of the quotient $v(z)u_2(z)/(u_1(z)z^{Qd})$ in case $s_M = 1, M = Q(d-1)$, but $\gamma = 0$ otherwise.

From this criterion we deduce the following consequence:

Corollary 3.2 *If $f \in \mathbb{C}[[z]] \setminus \mathbb{C}(z)$ satisfies $f(z^d) - f(z) \in \mathbb{C}(z)$, then f is hypertranscendental.*

Proof Let f, as in the corollary, satisfy $f(z^d) - f(z) \in \mathbb{C}(z), = v(z) \in \mathbb{C}[[z]]$, say, hence $v(0) = 0$. Assume that (i) from Theorem 3.1 holds. Since (ii) holds also, with $u(z) = 1$ (hence $M = 0, s_M = 1, Q = 0$) and $v(z)$ as above, there exists some $w \in \mathbb{C}(z)$ satisfying

$$w(z^d) = w(z) + v(z) \tag{3.1}$$

(as soon as we have checked $\gamma = 0$: $u_1(z) = 1; u_2 \in \mathbb{C}(z) \setminus \{0\}$ fulfills $u_2(z^d) = u_2(z)$, or $U(z^d)V(z) = U(z)V(z^d)$ with $u_2 = U/V, U, V \in \mathbb{C}[z] \setminus \{0\}$ coprime, whence $u_2 = \text{const} \in \mathbb{C}^\times$, and thus $\gamma = 0$).

By (3.1), $w(z)$ has no pole at 0, hence it is in $\mathbb{C}[[z]]$. Since f satisfies also (3.1), $\varphi := f - w \in \mathbb{C}[[z]]$ satisfies $\varphi(z^d) = \varphi(z)$, whence $\varphi = \text{const}$, and we arrive at the contradiction $f = w + \text{const} \in \mathbb{C}(z)$. □

In particular, all $G_d(z)$ and $F_d(z)$ are hypertranscendental.

To see what this implies arithmetically, we quote the following algebraic independence criterion:

Theorem 3.3 ([12, Theorem 4.2.1]) *Let K be an algebraic number field. Suppose that $f_1, \ldots, f_n \in K[[z]]$ converge in $|z| < \rho$ with some $0 < \rho \leq 1$, where they satisfy*

$$^\tau(f_1(z^d), \ldots, f_n(z^d)) = \mathcal{A}(z) \cdot {}^\tau(f_1(z), \ldots, f_n(z)) + {}^\tau(b_1(z), \ldots, b_n(z)) \tag{3.2}$$

with $\mathcal{A} \in \text{Mat}_{n\times n}(K(z)), b_1, \ldots, b_n \in K(z)$, and τ indicating the matrix transpose. If $\alpha \in \overline{\mathbb{Q}}^\times$ with $|\alpha| < \rho$ is such that no α^{d^j} $(j = 0, 1, \ldots)$ is a pole of $b_1, \ldots, b_n$ and

the entries of $\mathcal{A}$, then the following inequality holds for transcendence degrees

$$\operatorname{trdeg}_{\mathbb{Q}}\mathbb{Q}(f_1(\alpha),\dots,f_n(\alpha)) \geq \operatorname{trdeg}_{K(z)}K(z)(f_1(z),\dots,f_n(z)). \tag{3.3}$$

We apply this with $f_i(z) := f^{(i-1)}(z)$, f being an irrational solution of

$$f(z^d) = f(z) - H(z), \quad H = \frac{A}{B}, \tag{3.4}$$

with A, B as in our introduction [compare (1.2)]. According to Corollary 3.2, f is hypertranscendental, whence the right-hand side of (3.3) equals n for any $n \geq 1$. By successive differentiations of (3.4), we recognize

$$\tilde{\mathcal{A}}(z)\cdot {}^{\tau}(f(z^d),\dots,f^{(n-1)}(z^d)) = {}^{\tau}(f(z),\dots,f^{(n-1)}(z)) - {}^{\tau}(H(z),\dots,H^{(n-1)}(z))$$

with lower triangular $\tilde{\mathcal{A}}(z) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}[z])$ having $1, dz^{d-1},\dots,(dz^{d-1})^{n-1}$ on the main diagonal. From this, (3.2) can be easily checked with $\mathcal{A}(z) := \tilde{\mathcal{A}}(z)^{-1}$, ${}^{\tau}(b_1(z),\dots,b_n(z)) = -\mathcal{A}(z)\cdot {}^{\tau}(H(z),\dots,H^{(n-1)}(z))$. Clearly, $\mathcal{A}$ has no poles $\neq 0$, whereas non-zero poles of b_i can only come from zeros of B, and we have established the following result:

Corollary 3.4 *Suppose that f is an irrational solution of (3.4), where $A, B \in \overline{\mathbb{Q}}[z]\setminus\{0\}$. Then, for any $\alpha \in \overline{\mathbb{Q}}^{\times}$ with $|\alpha| < \min(1,\Delta)$ and $B(\alpha^{d^j}) \neq 0$ for $j = 0, 1,\dots$, the numbers $f(\alpha), f'(\alpha), f''(\alpha),\dots$ are algebraically independent.*

In particular, for any d and $\alpha \in \overline{\mathbb{Q}}^{\times}$, $|\alpha| < 1$, the numbers $G_d(\alpha), G_d'(\alpha), G_d''(\alpha),\dots$ are algebraically independent.

4 Algebraic Independence of the Values of Schwarz' Functions

The most typical question here is as follows. For a Mahler-type function f, analytic on $\mathbb{D} := \{z \in \mathbb{C} : |z| < 1\}$, say, one is interested in necessary and sufficient conditions on $\alpha_1,\dots,\alpha_n \in \overline{\mathbb{Q}}^{\times} \cap \mathbb{D}$ such that $f(\alpha_1),\dots,f(\alpha_n)$ are algebraically independent. This problem was essentially solved for the Fredholm series F_d, $d \geq 2$, by Loxton and van der Poorten [5]. But in the case of Schwarz' functions G_d, no significant results seem to exist in the literature, at least to our knowledge. We want to make here a modest contribution to this problem.

To begin with, we conclude analogously to [12, pp. 106–107] as follows. Suppose $\alpha_1,\dots,\alpha_n \in \overline{\mathbb{Q}}^{\times} \cap \mathbb{D}$ to be multiplicatively independent, and consider the multivariable functions $f_j(z_1,\dots,z_n) := G_d(z_j)$, $j = 1,\dots,n$. Since $G_d(z)$ is transcendental over $\mathbb{C}(z)$, the functions $f_1(\underline{z}),\dots,f_n(\underline{z})$ of the multivariable $\underline{z} := (z_1,\dots,z_n)$ are algebraically independent over $\mathbb{C}(\underline{z})$. Moreover, $\Omega := \mathrm{diag}(d,\dots,d) \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_{\geq 0})$ and $\underline{\alpha} := (\alpha_1,\dots,\alpha_n)$ satisfy the properties (I)

through (IV) from [12, pp. 33–34, 62], whence we obtain the algebraic independence of $G_d(\alpha_1), \ldots, G_d(\alpha_n)$ if, as assumed above, the numbers $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent. Note that the main feature here consists in the trick to deduce algebraic independence results for one single-valued function at different points from corresponding results on several multivariable functions at one point.

In a very particular subcase of multiplicatively dependent $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^\times \cap \mathbb{D}$, we are in a position to give a characterization of the algebraic independence of $G_d(\alpha_1), \ldots, G_d(\alpha_n)$, namely if all α_j's are powers of some $\alpha \in \overline{\mathbb{Q}}^\times \cap \mathbb{D}$.

Theorem 4.1 *Let $m_1, \ldots, m_n$ be $n \geq 2$ positive integers, and let $\alpha \in \overline{\mathbb{Q}}^\times \cap \mathbb{D}$. Then $G_d(\alpha^{m_1}), \ldots, G_d(\alpha^{m_n})$ are algebraically independent if and only if*

$$\frac{m_j}{m_i} \notin d^{\mathbb{Z}} \tag{4.1}$$

holds for any pair (i, j) with $i \neq j$.

To prepare our proof below, we next quote the one-variable version of a main tool for algebraic independence of Mahler-type functions.

Theorem 4.2 *Let $f_1, \ldots, f_n \in \mathbb{C}[[z]]$ satisfy the functional equation*

$$^\tau(f_1(z), \ldots, f_n(z)) = \mathcal{A} \cdot {}^\tau(f_1(z^d), \ldots, f_n(z^d)) + {}^\tau(b_1(z), \ldots, b_n(z)) \tag{4.2}$$

with $\mathcal{A} \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ and $b_1, \ldots, b_n \in \mathbb{C}(z)$. If $f_1, \ldots, f_n$ are algebraically dependent over $\mathbb{C}(z)$, then there exist $c_1, \ldots, c_n \in \mathbb{C}$, not all 0, such that $c_1 f_1 + \ldots + c_n f_n \in \mathbb{C}(z)$.

Proof This is a particular case of [12, Theorem 3.2.2], a forerunner of which was [4, Theorem 2].

Proof of Theorem 4.1 We consider the functions

$$f_j(z) := G_d(z^{m_j}) \quad (j = 1, \ldots, n) \tag{4.3}$$

satisfying, by (1.1),

$$f_j(z^d) = f_j(z) + \frac{z^{m_j}}{z^{m_j} - 1} \quad (j = 1, \ldots, n) \tag{4.4}$$

which is a system of functional equations of type (4.2). Iterating (4.4) we find

$$f_j(z^{d^\ell}) = f_j(z) + \sum_{\lambda=0}^{\ell-1} \frac{z^{d^\lambda m_j}}{z^{d^\lambda m_j} - 1}$$

for any integer $\ell \geq 0$, empty sums being 0, by convention. Assuming w.l.o.g. $m_2/m_1 = d^\ell$, this equation yields $G_d(\alpha^{m_2}) - G_d(\alpha^{m_1}) \in \overline{\mathbb{Q}}$, by (4.3), where the explicit value of this difference can be written down. Thus, the validity of (4.1) is necessary for the algebraic independence of $G_d(\alpha^{m_1}), \ldots, G_d(\alpha^{m_n})$.

That conditions (4.1) are sufficient for the algebraic independence of the numbers just mentioned can be deduced from Theorem 3.3 as follows: Applying this theorem with $K = \mathbb{Q}, \rho = 1$ and (4.4) as system (3.2), we obtain $\mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(f_1(\alpha), \ldots, f_n(\alpha)) \geq n$, by (3.3), hence our assertion, if we can show that our $f_1(z), \ldots, f_n(z)$ are algebraically independent over $\mathbb{Q}(z)$.

To prove even their algebraic independence over $\mathbb{C}(z)$, we use Theorem 4.2 which tells us the following. If $f_1, \ldots, f_n$ were algebraically dependent over $\mathbb{C}(z)$, then there exists a $\underline{c} := (c_1, \ldots, c_n) \in \mathbb{C}^n \setminus \{\underline{0}\}$ such that $r(z) := c_1 f_1(z) + \ldots + c_n f_n(z)$ is a rational function satisfying the functional equation

$$r(z^d) = r(z) + \sum_{j=1}^{n} c_j \frac{z^{m_j}}{z^{m_j} - 1}, \tag{4.5}$$

by (4.4).

To get our desired contradiction more conveniently, we next transform, for our above $\underline{c} \neq \underline{0}$, Eq. (4.5) in $r, m_1, \ldots, m_n$ into an equivalent one in $s, k_1, \ldots, k_n$. To this purpose we write, for $j = 1, \ldots, n$, $m_j = d^{t(j)} k_j$ with integers $t(j) \geq 0$ and $k_j > 0$ such that $d \nmid k_j$. Then condition (4.1) is equivalent to the distinctness of $k_1, \ldots, k_n$. Moreover, with $\underline{c}$ and r as in (4.5), we define the rational function s by

$$s(z) := r(z) - \sum_{j=1}^{n} c_j \sum_{\tau=0}^{t(j)-1} \frac{z^{d^\tau k_j}}{z^{d^\tau k_j} - 1}$$

which satisfies

$$s(z^d) = s(z) + \sum_{j=1}^{n} c_j \frac{z^{k_j}}{z^{k_j} - 1}. \tag{4.6}$$

Therefore, to reach our contradiction, it suffices to establish the following auxiliary result the proof of which we defer to the last section. □

Lemma 4.3 *If $\underline{c} := (c_1, \ldots, c_n) \in \mathbb{C}^n \setminus \{\underline{0}\}$, and $k_1, \ldots, k_n$ are distinct positive integers not divisible by d, then the functional equation (4.6) has no rational solution s.*

This may be the right place to ask an

Open Question *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^\times \cap \mathbb{D}$. Are the following two statements equivalent?*

(i) *$G_d(\alpha_1), \ldots, G_d(\alpha_n)$ are algebraically independent.*
(ii) *$\alpha_j \neq \alpha_i^{d^\ell}$ holds for any triple (i, j, ℓ) with $i \neq j$ and $\ell \geq 0$.*

Of course, the implication (i) $\Rightarrow$ (ii) is easily seen. In the particular case $\alpha_j = \alpha^{m_j}$ treated in Theorem 4.1, the reversed implication is also valid.

5 Proof of Lemma 4.3

Step 1: *Partial fraction decomposition*. Assume on the contrary, that, for a $(c_1, \ldots, c_n) \neq \underline{0}$, Eq. (4.6) with distinct k_j not divisible by d has a rational solution s. Since all polynomials $z^{k_j} - 1$ divide $z^L - 1$, $L := \operatorname{lcm}(k_1, \ldots, k_n)$, it follows from [13, Lemma 1] that s must be of the shape

$$s(z) = \frac{a(z)}{z^L - 1}$$

with some $a \in \mathbb{C}[z]$, $a \neq 0$, by (4.6) and the distinctness of the k_j. Note also $\deg a \leq L$.

For integers $k > 0$, we write $\zeta_k := e^{2\pi i/k}$ and have

$$\frac{z^k}{z^k - 1} = 1 + \frac{1}{k} \sum_{j=0}^{k-1} \frac{\zeta_k^j}{z - \zeta_k^j} = 1 + \frac{1}{k} \sum_{\delta | k} f_\delta(z),$$

the second sum being over all positive divisors δ of k, where we put

$$f_\delta(z) := \sum_{\substack{j=0 \\ (j,\delta)=1}}^{\delta-1} \frac{\zeta_\delta^j}{z - \zeta_\delta^j}.$$

Here the poles of f_δ are exactly the primitive δth roots of unity, i.e., the roots of the δth cyclotomic polynomial.

In the same way, we may write down the partial fraction decomposition of s as

$$s(z) = S + \sum_{\delta | L} s_\delta(z) \quad \text{with} \quad s_\delta(z) := \sum_{\substack{j=0 \\ (j,\delta)=1}}^{\delta-1} \frac{s_{\delta,j}}{z - \zeta_\delta^j},$$

where S and the $s_{\delta,j}$'s are complex constants.

By the preceding notations, our functional equation (4.6) assumes the form

$$\sum_{\delta | L} \left(s_\delta(z^d) - s_\delta(z) \right) = \sum_{j=1}^{n} \frac{c_j}{k_j} \sum_{\delta | k_j} f_\delta(z), \tag{5.1}$$

where we already used $c_1 + \ldots + c_n = 0$, a result coming from the fact that both sides of (5.1) tend to 0 as $z \to \infty$. W.l.o.g., let us assume $c_1 \cdot \ldots \cdot c_m \neq 0$ but $c_{m+1} = \ldots = c_n = 0$ for $2 \leq m \leq n$, and furthermore $k_1 > \ldots > k_m$. Next, consider the set of all positive integers δ dividing at least one of $k_1, \ldots, k_m$, where none of these δ's is divisible by d since we assumed $d \nmid k_j$ for $j = 1, \ldots, n$. Clearly k_1 is the maximal

element of this set and cannot occur among the divisors of $k_2, \dots, k_m$. Thus, all poles of f_{k_1} remain poles of the right-hand side of (5.1), and we may summarize the result of Step 1 as follows: Denoting by N the greatest positive integer such that the left-hand side

$$\sum_{\delta | L} \big(s_\delta(z^d) - s_\delta(z)\big) \tag{5.2}$$

of (5.1) and f_N have at least one pole in common, then $N = k_1$ holds, whence $d \nmid N$.

Step 2: *Study of $s_\delta(z^d)$ and final contradiction*. From the above definition of s_δ for positive divisors δ of L we obtain

$$s_\delta(z^d) = \sum_{\substack{j=0 \\ (j,\delta)=1}}^{\delta-1} \frac{s_{\delta,j}}{z^d - \zeta_\delta^j} = \sum_{\substack{j=0 \\ (j,\delta)=1}}^{\delta-1} s_{\delta,j} \sum_{\kappa=0}^{d-1} \frac{1}{d\zeta_{d\delta}^{(j+\kappa\delta)(d-1)}(z - \zeta_{d\delta}^{j+\kappa\delta})}. \tag{5.3}$$

Suppose, from now on, $p_1^{\nu(1)} \cdot \ldots \cdot p_\omega^{\nu(\omega)}$ to be the canonical factorization of d. Assume that $p_1, \dots, p_\sigma$ are not divisors of δ but $p_{\sigma+1}, \dots, p_\omega$ are, where we have to consider the cases $\sigma = 0, \dots, \omega$. Then we have the following equivalence:

$$(j, \delta) = 1 \iff (j + \kappa\delta, \delta) = (j + \kappa\delta, d\delta / \textstyle\prod_{i=1}^{\sigma} p_i^{\nu(i)}) = 1$$

with the usual convention here and later that empty products equal 1. Now, any positive divisor D of $p_1 \cdot \ldots \cdot p_\sigma$ is relatively prime to δ, whence there are precisely $\frac{d}{D}$ numbers $\kappa \in \{0, \dots, d-1\}$ satisfying $D | (j + \kappa\delta)$. Thus, by the well-known inclusion–exclusion principle, we can say that, for fixed coprime j, δ, the number of $\kappa \in \{0, \dots, d-1\}$ such that $j + \kappa\delta$ is prime to $p_1 \cdot \ldots \cdot p_\sigma$ (or equivalently to $\prod_{i=1}^{\sigma} p_i^{\nu(i)}$) equals $d \prod_{i=1}^{\sigma}(1 - 1/p_i)$. Therefore we can note that, for fixed coprime j, δ, there are exactly $d \prod_{i=1}^{\sigma}(1 - 1/p_i)$ values $\kappa \in \{0, \dots, d-1\}$ such that $(j + \kappa\delta, d\delta) = 1$ holds. Hence we conclude

$$s_\delta(z^d) = \sum_{\substack{j=0 \\ (j,d\delta)=1}}^{d\delta-1} \frac{s_{\delta,j}}{d\zeta_{d\delta}^{j(d-1)}(z - \zeta_{d\delta}^j)} + \Sigma_\delta(z) \tag{5.4}$$

from the double sum in (5.3), where, strictly speaking, we should write $s_{\delta, j-[j/\delta]\delta}$ in the numerator instead of simply $s_{\delta,j}$. The rational function Σ_δ in (5.4) vanishes identically in case $\sigma = 0$, whereas, in the cases $1 \le \sigma \le \omega$, it may have poles at certain primitive ρth roots of unity but with $\rho < d\delta$ only. Since $s_\delta \not\equiv 0$ is equivalent to the fact that not all $s_{\delta,j}, j \in \{0, \dots, d\delta - 1\}$ and prime to $d\delta$, vanish, we conclude from (5.4) that, in this case of δ, the difference $s_\delta(z^d) - s_\delta(z)$ has poles at $(d\delta)$th roots of unity. Thus, the N defined before (5.2) must be of the form $d\delta$, whence $d | N$ holds, and we have obtained a contradiction proving Lemma 4.3.

References

1. P. Bundschuh, K. Väänänen, Algebraic independence of certain Mahler functions and of their values. J. Aust. Math. Soc. **98**, 289–310 (2015)
2. M. Coons, Extension of some theorems of W. Schwarz. Can. Math. Bull. **55**, 60–66 (2012)
3. D. Duverney, Ku. Nishioka, An inductive method for proving transcendence of certain series. Acta Arith. **110**, 305–330 (2003)
4. J.H. Loxton, A.J. van der Poorten, A class of hypertranscendental functions. Aequationes Math. **16**, 93–106 (1977)
5. J.H. Loxton, A.J. van der Poorten, Algebraic independence properties of the Fredholm series. J. Aust. Math. Soc. Ser. A **26**, 31–45 (1978)
6. K. Mahler, Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen. Math. Ann. **101**, 342–366 (1929); Berichtigung, ibid. **103**, 532 (1930)
7. K. Mahler, Über das Verschwinden von Potenzreihen mehrerer Veränderlicher in speziellen Punktfolgen. Math. Ann. **103**, 573–587 (1930)
8. K. Mahler, Arithmetische Eigenschaften einer Klasse transzendental-transzendenter Funktionen. Math. Z. **32**, 545–585 (1930)
9. K. Mahler, Remarks on a paper by W. Schwarz. J. Number Theory **1**, 512–521 (1969)
10. Ke. Nishioka, A note on differentially algebraic solutions of first order linear difference equations. Aequationes Math. **27**, 32–48 (1984)
11. Ke. Nishioka, Algebraic function solutions of a certain class of functional equations. Arch. Math. **44**, 330–335 (1985)
12. Ku. Nishioka, *Mahler Functions and Transcendence*. Lecture Notes in Mathematics, vol. 1631 (Springer, Berlin, 1996)
13. Ku. Nishioka, Algebraic independence of reciprocal sums of binary recurrences. Monatsh. Math. **123**, 135–148 (1997)
14. W. Schwarz, Remarks on the irrationality and transcendence of certain series. Math. Scand. **20**, 269–274 (1967)

Sums of Two Squares and a Power

Rainer Dietmann and Christian Elsholtz

Dedicated to the memory of Wolfgang Schwarz, with admiration for his broad interests, inside and outside mathematics.

Abstract We extend results of Jagy and Kaplansky and the present authors and show that for all $k \geq 3$ there are infinitely many positive integers n, which cannot be written as $x^2 + y^2 + z^k = n$ for positive integers x, y, z, where for $k \not\equiv 0 \bmod 4$ a congruence condition is imposed on z. These examples are of interest as there is no congruence obstruction itself for the representation of these n. This way we provide a new family of counterexamples to the Hasse principle or strong approximation.

Keywords Hasse principle • Strong approximation • Ternary additive problems • Waring type problems

2010 Mathematics subject classification: Primary 11E25; Secondary 11P05

1 Introduction

This paper is dedicated to the memory of Wolfgang Schwarz, who was the PhD advisor of the second named author. In particular Wolfgang Schwarz's books "Einführung in Siebmethoden der analytischen Zahlentheorie" and "Arithmetical functions" were very useful for the second author's own studies.

R. Dietmann
Department of Mathematics, Royal Holloway, University of London, Egham TW20 0EX, UK
e-mail: Rainer.Dietmann@rhul.ac.uk

Ch. Elsholtz (✉)
Institut für Mathematik und Zahlentheorie, Technische Universität Graz,
Kopernikusgasse 24/II, A-8010 Graz, Austria
e-mail: elsholtz@math.tugraz.at

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_7

Looking at Schwarz's own PhD thesis, see [11, 12], which is on sums of prime powers, i.e. on the Goldbach–Waring problem, one finds a great number of results, one of those being the following (Theorem 3 of [12]):

For fixed $k \geq 1$ let $S_k(N)$ be the set of positive integers n, with

$$\begin{array}{ll} 3 \leq n \leq N, & \\ n \not\equiv 0 \bmod 2, \ n \not\equiv 2 \bmod 3, & \text{for odd } k \\ n \equiv 3 \bmod 24, & \text{for even } k, \\ n \not\equiv 0 \bmod 5, & \text{for } k \equiv 2 \bmod 4 \\ n \not\equiv 0, 2 \bmod 5, & \text{for } k \equiv 0 \bmod 4 \\ n \not\equiv 1 \bmod p, & \text{for each } p \equiv 3 \bmod 4 \text{ with } (p-1) \mid k. \end{array}$$

Then the number of integers $n \in S_k(N)$ not of the form

$$n = p_1^2 + p_2^2 + p_3^k,$$

is, for all $B > 0$, at most

$$O_B\left(\frac{N}{(\log N)^B}\right).$$

This improved on a result of Hua [8, Theorem 1], who proved this with $B = \frac{k}{k+2}$. As we had worked earlier on solutions of $x^2 + y^2 + z^k = n$, it is due to this connection that we have chosen to contribute the present note to the volume in Memory of Wolfgang Schwarz.

As it turns out, also one of the first named author's PhD advisors worked on this kind of problem in his PhD thesis: without restricting the variables to primes, one should be able to obtain stronger results, and indeed, improving on earlier work pioneered by Davenport and Heilbronn [3] and further developed by many other authors, Brüdern [1] has shown that there are at most $O(N^{1-\frac{1}{k}+\epsilon})$ integers $n \leq N$ with no solutions of

$$n = x^2 + y^2 + z^k, \tag{1.1}$$

where n is not in a residue class excluded by congruence obstructions. For a survey of results on sums of mixed powers, see also [2] and [14].

It was generally expected that for all sufficiently large n the Hasse principle for Eq. (1.1) holds true, i.e. for all such n satisfying the necessary congruence conditions there would exist a solution of (1.1) in positive integers, see, for example, Chap. 8 in [13]. However, in 1995 Jagy and Kaplansky [9] shattered this belief by proving that for $k = 9$ and some positive constant c there are at least $c\frac{N^{1/3}}{\log N}$ positive integers $n \leq N$ that are not sums of two squares and one kth power. In fact, their method works for any odd composite number k, but not for the other cases of k. In [4] we proved that a similar restriction holds for $k = 4$. That approach actually generalizes

to all k divisible by four (see Theorem 3.1), and by slightly modifying it we can not only get a bigger set of exceptional n but we can also handle k not divisible by four; to be more specific, we prove that (1.1) does not satisfy 'strong approximation': For $k \equiv 2 \pmod 4$, $k \geq 6$ and sufficiently large N we show that there are asymptotically $\gg N^{1/2}/(\log N)^{1/2}$ positive integers $n \leq N$ for which Eq. (1.1) has no solution with z fixed into a certain residue class, though there are no congruence obstructions (see Theorem 3.2). For odd $k \geq 3$ we show that there are asymptotically at least $\frac{kN^{1/k}}{2\varphi(k)\log N}$ such exceptional positive integers $n \leq N$ (see Theorem 2.1).

Let us further mention that Hooley [7] investigated sums of three squares and a kth power, Friedlander and Wooley [5] sums of two squares and three biquadrates, and Wooley [15] sums of squares and a 'micro square', in connection with a conjecture of Linnik. In this connection we would like to add a seemingly forgotten old reference: Theorem 7 of Rieger [10] states that the number of integers $n \leq N$ which can be written as $n = x^2 + y^2 + z^k$, where $z \leq F(N)$, and F is a function tending monotonically to infinity, with $F(n) \leq \sqrt{\log N}$, is $\gg_{k,F} \frac{N F(N)}{\sqrt{\log N}}$, in other words, as good as it can be.

The authors are grateful to Tim Browning, Jörg Brüdern, Roger Heath-Brown, Jan-Christoph Schlage-Puchta, Dasheng Wei and Trevor Wooley for interesting discussions or observations.

2 Two Squares and an Odd kth Power

Theorem 2.1 *Let $k \geq 3$ be odd. Let p be a prime with $p \equiv 1 \bmod 4k$. Then there are no integers x, y, z, positive or negative, with $x^2 + y^2 + z^k = p^k$ and $z \equiv 2k \bmod 4k$.*

Proof Assume there are solutions, then $x^2 + y^2 = (p - z)(p^{k-1} + p^{k-2}z + \cdots + pz^{k-2} + z^{k-1})$. If $z \equiv 2k \bmod 4k$, then $p - z \equiv 2k + 1 \bmod 4k$. Since k is odd, $2k + 1 \equiv 3 \bmod 4$. Hence $p - z$ must contain a prime divisor $q \equiv 3 \bmod 4$ with odd multiplicity. Note that $\gcd(q, k) = 1$, as otherwise $q|k$ and $0 \equiv p - z \equiv 2k + 1 \equiv 1 \bmod q$ gives a contradiction.

Recall that by the general classification of integers which are sums of two squares the integer $x^2 + y^2$ contains prime factors $q \equiv 3 \bmod 4$ with even multiplicity only. Therefore both $p - z$ and $p^{k-1} + p^{k-2}z + \cdots + pz^{k-2} + z^{k-1}$ are divisible by q. With $p \equiv z \bmod q$ it follows that

$$p^{k-1} + p^{k-2}z + \cdots + pz^{k-2} + z^{k-1} \equiv kz^{k-1} \equiv 0 \bmod q.$$

This implies that $q \mid z$ and hence $q \mid p$, which is impossible, as $q = p$ would contradict $p \equiv 1 \bmod 4$.

Also note that there are no congruence obstructions that would imply that in $x^2 + y^2 + z^k = p^k$ there are no solutions with $z \equiv 2k \bmod 4k$.

To see this first observe that for a fixed odd prime q one can choose an integer $z \equiv 2k \bmod 4k$ such that q is coprime to $p^k - z^k$; similarly, for $q = 8$ just choose

$z = 2k$. For this fixed z the congruence $x^2 + y^2 + z^k \equiv p^k \bmod q$ has a nonsingular solution in x and y which by Hensel's lemma can be lifted to a q-adic or 2-adic solution, respectively.

By the prime number theorem in arithmetic progressions, the number of such examples, $p^k \le N$ with $p \equiv 1 \bmod 4k$, is asymptotically

$$\frac{1}{\varphi(4k)} \int_2^{N^{1/k}} \frac{dt}{\log t} \sim \frac{k}{2\varphi(k)} \frac{N^{1/k}}{\log N}.$$

3 Two Squares and an Even *k*th Power

3.1 Two Squares and a kth Power, $k \equiv 0 \bmod 4$

Theorem 3.1 *Suppose that* $4 \mid k$ *and let* p *be a prime with* $p \equiv 7 \bmod 8$. *Let* $n \equiv 1 \bmod 8$ *be either* 1 *or consist of prime factors congruent to* 1 mod 4 *only, and assume that* $n < p$. *Then there are no positive integers* x, y, z *with* $x^2 + y^2 + z^k = (np)^2$.

Proof Let $k = 2t$, where t is even. Assume there are solutions, then $x^2 + y^2 = (np - z^t)(np + z^t)$. If z is even, then $np - z^t \equiv 3 \bmod 4$. If z is odd, then $np - z^t \equiv 6 \bmod 8$. In both cases $np - z^t$ must contain a prime divisor $q \equiv 3 \bmod 4$ with odd multiplicity. Therefore, as in the proof of Theorem 2.1, we conclude that both $np - z^t$ and $np + z^t$ are divisible by q. Hence their sum $2np$ and their difference $-2z^t$ are also divisible by q. Since $2n \not\equiv 0 \bmod q$, and since p is prime: $p = q$, and since $z \neq 0$: q divides z. But this gives a contradiction:

$$x^2 + y^2 + z^k > q^k \ge q^4 > (nq)^2 = (np)^2.$$

Let us give an estimate of the number of integers $np \le N$, with $n \equiv 1 \bmod 8$ consisting of prime factors 1 mod 4 only, and $n < p$.

Recall that by a theorem of Landau the number of integers $n \le N$ consisting of prime factors 1 mod 4 only is of order of magnitude $\frac{N}{(\log N)^{1/2}}$, and about one half of these numbers satisfy the congruence restriction $n \equiv 1 \bmod 8$.

Let $f : \mathbb{N} \to \{0, 1\}$ be the characteristic function of these integers n, i.e. we put $f(n) = 1$, if $n \equiv 1 \bmod 8$, and all prime factors of n are 1 mod 4; otherwise, we put $f(n) = 0$. Now

$$\sum_{np \le N, n < p} f(n) = \sum_{n \le N/p, n < p} f(n) \gg \sum_{N^{1/2} \le p \le N^{3/4}} \frac{N/p}{(\log(N/p))^{1/2}} \gg \frac{N}{(\log N)^{1/2}},$$

where we used that

$$\sum_{N^{1/2}\le p\le N^{3/4}} \frac{1}{p} = \log\log N^{3/4} - \log\log N^{1/2} + o(1) = \log(3/2) + o(1) \gg 1.$$

(In view of Landau's theorem this order is the right order of magnitude.) Hence the number of exceptional $(np)^2 \le N$ provided by Theorem 3.1 is $\gg \frac{N^{1/2}}{(\log N)^{1/2}}$.

Note that as for Theorem 2.1 one can check that there are no congruence obstructions for the representation of $(np)^2$.

3.2 *Two Squares and a kth Power, $k \equiv 2 \bmod 4$*

Theorem 3.2 *Suppose that $k \equiv 2 \bmod 4$, $k \ge 6$ and let p be a prime with $p \equiv 7 \bmod 8$. Let $n < p$ be an integer either 1 or consisting of prime factors congruent to 1 mod 4 only, and $n \equiv 1 \bmod 8$. Then there are no positive integers x, y, z, where $2 \mid z$, with $x^2 + y^2 + z^k = (np)^2$.*

Proof The proof is almost verbatim as above.

Let us remark that as above one shows that the number of exceptional $(np)^2 \le N$ provided by Theorem 3.2 is $\gg \frac{N^{1/2}}{(\log N)^{1/2}}$. Further note that in a similar way as for Theorem 2.1 one observes that there are no congruence obstructions for the requested representation of $(np)^2$.

4 Afterthought

A major part of the paper was actually written around 2007/2008. We had shown earlier versions of this paper to several colleagues, hoping that someone would write a more detailed explanation based on tools from arithmetic geometry such as the Brauer–Manin obstruction. Indeed, in this way the question has come to Fabian Gundlach [6] who was very recently able to give a detailed and general account.

As Gundlach refers to our work as an unpublished manuscript, and as our proofs use a much less sophisticated language, it seems desirable to have this paper in final form. The main part of this paper is a slightly improved version, compared to the manuscript Gundlach referred to. In particular, the version cited by Gundlach [6] had in Theorem 2.1 the same statement and proof with p^{2k} rather than p^k. Also in Theorems 3.1 and 3.2 we now have an additional factor n, thanks to an observation of J.C. Schlage-Puchta. In other words, the current version gives slightly stronger results.

References

1. J. Brüdern, Iterationsmethoden in der additiven Zahlentheorie. Dissertation, Universität Göttingen, 1988
2. J. Brüdern, K. Kawada, Ternary problems in additive prime number theory, in *Analytic Number Theory (Beijing/Kyoto, 1999)*. Developments in Mathematics, vol. 6 (Kluwer, Dordrecht, 2002), pp. 39–91
3. H. Davenport, H. Heilbronn, Note on a result in the additive theory of numbers. Proc. Lond. Math. Soc. **43**, 142–151 (1937)
4. R. Dietmann, C. Elsholtz, Sums of two squares and one biquadrate. Funct. Approx. Comment. Math. **38**(2), 233–234 (2008)
5. J.B. Friedlander, T.D. Wooley, On Waring's problem: two squares and three biquadrates. Mathematika **60**(1), 153–165 (2014)
6. F. Gundlach, Integral Brauer-Manin obstructions for sums of two squares and a power. J. Lond. Math. Soc. (2) **88**(2), 599–618 (2013)
7. C. Hooley, On Waring's problem for three squares and an ℓth power. Asian J. Math. **4**(4), 885–904 (2000)
8. L.-K. Hua, Some results in the additive prime number theory. Q. J. Math. **9**(1), 68–80 (1938)
9. W.C. Jagy, I. Kaplansky, Sums of squares, cubes, and higher powers. Exp. Math. **4**(3), 169–173 (1995)
10. G.J. Rieger, Anwendung der Siebmethode auf einige Fragen der additiven Zahlentheorie. I. J. Reine Angew. Math. **214/215**, 373–385 (1964)
11. W. Schwarz, Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. I. Darstellung hinreichend grosser Zahlen. J. Reine Angew. Math. **205**, 21–47 (1960/1961)
12. W. Schwarz, Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. II. J. Reine Angew. Math. **206**, 78–112 (1961)
13. R.C. Vaughan, *The Hardy-Littlewood Method*, 2nd edn. (Cambridge University Press, Cambridge, 1997)
14. R.C. Vaughan, T.D. Wooley, Waring's problem: a survey, in *Number Theory for the Millennium, III (Urbana, IL, 2000)* (A K Peters, Natick, 2002), pp. 301–340
15. T.D. Wooley, On Linnik's conjecture: sums of squares and microsquares. Int. Math. Res. Not. **2014**(20), 5713–5736 (2014)

Multiplicative Functions and the Sign of Maass Form Fourier Coefficients

Peter D.T.A. Elliott

In memory of Wolfgang Schwarz

Abstract Mean value theorems for multiplicative arithmetic functions are applied to demonstrate uniformity of sign changes in the Fourier coefficients of automorphic forms.

Keywords Maass form • Mean value • Multiplicative function

2010 Mathematics subject classification: Primary 11N37; Secondary 11F03, 11F30, 11K65, 11L99, 11M99, 11N60, 11N64

1 Introduction and Background

Wolfgang Schwarz' serious interest in the theory of multiplicative functions is well illustrated in the wonderfully wideranging 1994 volume *Arithmetical Functions* that, together with Jürgen Spilker, he wrote for the London Mathematical Society Lecture Note Series [9].

Classical multiplicative functions are usually supported on almost all the primes. In the present paper I consider multiplicative functions that may have scattered values and slender support, and apply them to establish uniform distribution of sign changes in real Fourier coefficients of automorphic cusp forms.

P.D.T.A. Elliott (✉)
Department of Mathematics, University of Colorado Boulder, Boulder, CO 80309-0395, USA
e-mail: pdtae@euclid.colorado.edu

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_8

We begin with the following result of Elliott and Kish [4].

Theorem 1 *Let $3/2 \le Y \le x$. Let g be a complex-valued multiplicative function that for positive constants β, c, c_1 satisfies $|g(p)| \le \beta$,*

$$\sum_{w<p\le x} (|g(p)| - c)\, p^{-1} \ge -c_1, \quad Y \le w \le x,$$

on the primes. Suppose, further, that the series

$$\sum_q |g(q)| q^{-1} (\log q)^{\kappa}, \quad \kappa = 1 + c\beta(c+\beta)^{-1},$$

taken over the prime-powers $q = p^k$ with $k \ge 2$, converges.

Then with

$$\Lambda = \min_{|t|\le T} \sum_{Y<p\le x} \left(|g(p)| - Re\, g(p) p^{it}\right) p^{-1},$$

$$\sum_{n\le x} g(n) \ll x(\log x)^{-1} \prod_{p\le x} \left(1 + |g(p)|p^{-1}\right) \left(\exp(-\Lambda c(c+\beta)^{-1}) + T^{-1/2}\right)$$

uniformly for Y, x, $T > 0$, the implied constant depending at most upon β, c, c_1 and a bound for the sum of the series over prime-powers.

Remark Since the partial sums $\sum_{p\le x} \left(|g(p)| - \mathrm{Re}\, g(p) p^{it}\right) p^{-1}$ are continuous in t and non-decreasing in x, their divergence for each real t ensures that

$$\sum_{n\le x} g(n) = o\left(x(\log x)^{-1} \prod_{p\le x} \left(1 + |g(p)|p^{-1}\right) \right), \quad x \to \infty.$$

Specialising:

Theorem 2 *Let g be a real-valued multiplicative function that satisfies the conditions on $g(p)$ in Theorem 1 for $Y = 3/2$ and all $x \ge 2$, and for which the series $\sum (|g(p)| - g(p))\, p^{-1}$ diverges.*

Then the asymptotic estimate in the above remark holds.

Further specialising, we obtain a result that I shall directly employ.

Theorem 3 *Let the multiplicative function g assume values 0, 1, -1, and with positive constants c, c_1 satisfy*

$$\sum_{u<p\le v} (|g(p)| - c)\, p^{-1} \ge -c_1,$$

uniformly for $2 \le u \le v$. *Assume, further, that the series* $\sum p^{-1}$, *taken over the primes for which* $g(p) = -1$, *diverges.*

Then

$$\sum_{n \le x} g(n) = o\left(x(\log x)^{-1} \prod_{p \le x} \left(1 + |g(p)|p^{-1}\right)\right), \quad x \to \infty.$$

Remark Integration by parts shows the lower bound hypothesis on $|g(p)|$ in Theorem 1, likewise in Theorems 2 and 3, to be amply satisfied if $\sum_{p \le x} |g(p)|p^{-1} \log p \ge c \log x - c_2$ for some $c_2 > 0$ and all $x \ge 2$.

Proof of Theorem 1 A complete proof of Theorem 1 may be found in Elliott and Kish [3, Theorem 2].

It is shown in Elliott and Kish [3, Lemma 14], that for a certain constant c_3 and t real,

$$\operatorname{Re} \sum_{2<p \le x} p^{-1-it} \le \begin{cases} 2 \log\log(2 + |t|) + c_3, & |t| \log 2 > 1, \\ -\log|t| + c_3, & (\log x)^{-1} < |t| \le (\log 2)^{-1}, \\ \log\log x + c_3, & |t| \log x \le 1, \end{cases}$$

uniformly for $x \ge 2$.

Denote this upper bound by $\theta(t)$ and let $L = \sum_{2<p \le x} p^{-1}$. To deduce Theorem 2 we shall apply the following result, a special case of Elliott and Kish [3, Lemma 15].

Lemma 1 *If for some* δ, $0 < \delta < 1$, t *real with* $h(p)$ *in the interval* $[0, 1]$,

$$\sum_{2<p \le x} h(p)p^{-1}|1 - p^{it}|^2 \le \delta L,$$

then

$$\sum_{2<p \le x} h(p)p^{-1} \le 4\delta^{1/3}L + 3\theta(2\delta^{-1/3}t) + 3\theta(t).$$

Proof of Theorem 2 Assume that for a non-zero real t the series $\sum (|g(p)| - \operatorname{Re} g(p)\, p^{it})\, p^{-1}$ converges. For z in the complex unit disc $|1 - z|^2 \le 2(1 - \operatorname{Re} z)$, and the partial sums $\sum_{2<p \le x} |g(p)||1 - p^{it}|^2$, $x \ge 2$, are uniformly bounded.

We may apply Lemma 1 with $h(p) = \beta^{-1}|g(p)|$ and $4\delta^{1/3} = c/2$. In view of our lower bound hypothesis on the values of $|g(p)|$, $\log\log x \ll \theta(2\delta^{-1/3}t) + \theta(t)$ which, for all sufficiently large values of x, is untenable.

We may now apply Theorem 1.

We may appreciate Theorem 2 by recalling two results of Wirsing [10].

Satz 1.1 *Let $\lambda(n)$ be a non-negative real-valued multiplicative function that for a positive τ satisfies*

$$\sum_{p\le x}\frac{\log p}{p}\lambda(p)\sim\tau\log x,\quad x\to\infty.$$

Let the $\lambda(p)$ be uniformly bounded and the series $\sum\lambda(q)q^{-1}$, taken over the prime-powers $q=p^k$ with $k\ge 2$, converge. Moreover, if $\tau\le 1$ then, with the same convention, let $\sum_{q\le x}\lambda(q)\ll x(\log x)^{-1}$ hold.

Then

$$\sum_{n\le x}\lambda(n)\sim\frac{e^{-\gamma t}}{\Gamma(\tau)}\frac{x}{\log x}\prod_{p\le x}\left(1+\frac{\lambda(p)}{p}+\frac{\lambda(p^2)}{p^2}+\cdots\right),\quad x\to\infty,$$

where γ denotes Euler's constant.

Satz 1.2.2 *Let $\lambda(n)$ satisfy the conditions of Satz 1.1, and let $g(n)$ be a real-valued multiplicative function that satisfies $|g(n)|\le\lambda(n)$ on the positive integers.*

Then

$$\lim_{x\to\infty}\sum_{n\le x}g(n)\left(\sum_{n\le x}\lambda(n)\right)^{-1}=\prod_p\left(1+\sum_{k=1}^{\infty}g(p^k)p^{-k}\right)\left(1+\sum_{k=1}^{\infty}\lambda(p^k)p^{-k}\right)^{-1},$$

where the product either converges properly to a non-zero limit, or improperly to zero.

If, for $0<\alpha<\beta$, we define the multiplicative function λ to be α,β on the primes in alternate intervals $\left[\exp(2^k),\exp(2^{k+1})\right)$, $k=-1,0,1,2,\dots$, and to be zero on all other prime-powers, then, as x increases through values $\exp(2^m)$,

$$(\log x)^{-1}\sum_{p\le x}p^{-1}g(p)\log p$$

approaches $(\alpha+2\beta)/3$ or $(\beta+2\alpha)/3$ according to whether m is confined to odd or to even integers.

Satz 1.1 and Satz 1.2.2 are then not applicable.

None-the-less, it is clear from Theorem 2 that for the multiplicative function g defined to be $-\alpha$ on those primes for which $\lambda(p)=\alpha$, and to coincide with λ on the remaining prime-powers, the conclusion of Satz 1.2.2 still holds. We do not need an asymptotic estimate for the mean of $\lambda(n)$, only an appropriate lower bound; and that can be provided by the following basic result.

Lemma 2 *Let g be a non-zero, non-negative real multiplicative function, uniformly bounded on the primes and for which the series $\sum g(q)q^{-1}$, taken over the prime-powers $q=p^k$ with $k\ge 2$, converges.*

Assume, further, that for a positive d and all sufficiently large x, $\sum_{p\le x} g(p)\log p \ge dx$.

Then $\sum_{n\le x} g(n)$ lies between positive constant multiples of

$$\frac{x}{\log x}\prod_{p\le x}\left(1+\sum_{k=1}^{\infty}\frac{g(p^k)}{p^k}\right)$$

uniformly for $x \ge 2$.

Proof of Lemma 2 c.f. Elliott and Kish [4, Lemmas 19, 20 and 21].

With $\tau = 1$, Satz 1.2.2 of Wirsing settled in the affirmative a conjecture, ascribed to Wintner and Erdős, that for a multiplicative function g that assumes values 0, 1, -1, the limit $\lim_{x\to\infty} x^{-1}\sum_{n\le x} g(n)$ always exists. Of particular interest was the case when g is Möbius' function μ since, as was already known to Landau at the beginning of the twentieth century, its validity led rapidly, and by elementary steps, to a proof of the rational prime number theorem.

Supposing the conclusion of Theorem 2 or 3 to be valid, it is not clear what more might be needed to guarantee even a weak estimate $\sum_{p\le x} |g(p)|p^{-1}\log p \sim \tau \log x$, $x\to\infty$, on the primes.

2 Application

Let

$$f = \sum_{n\ne 0} a_n (2\pi y)^{1/2} K_w(2\pi|n|y) e^{2\pi i n x}$$

be a Maass cusp form, a newform for the action of the congruence group $\Gamma_0(N)$ upon the complex upper half-plane H with trivial character, an eigenvector of the appropriate Hecke operators and normalised to have $a_1 = 1$; a solution to the Laplacian equation

$$-y^2\left(\frac{\partial^2 f}{\partial x^2}+\frac{\partial^2 f}{\partial y^2}\right) = \left(\frac{1}{4}-w^2\right)f$$

that belongs to the Hilbert space $L^2(\Gamma_0(N)\backslash H)$ with Petersson inner product.

We identify f with a cusp form attached to an irreducible cuspidal automorphic representation of $GL_2(A_{\mathbb{Q}})$, $A_{\mathbb{Q}}$ the rational adèles. We assume the representation to have trivial central character and not to be of dihedral, tetrahedral or octahedral type, c.f. Kim and Shahidi [7].

Let M be a finite collection of places including the archimedean and the non-archimedean whose local representation is ramified. Let D be the product of the corresponding rational primes. I shall deem the rational primes not dividing D to be unramified.

For $k = 1, 2, \dots$, denote by $L(s, \mathrm{sym}^k)$ the L-function attached to the extension of the representation onto symmetric tensors of rank k, and by $L_M(s, \mathrm{sym}^k)$ its Euler product restricted to unramified primes.

Let $\sum_{n=1}^{\infty} b_n n^{-s}$, for $\mathrm{Re}(s)$ sufficiently large, be one of the restricted L-functions, $L_M(s, \mathrm{sym}^k)$, $k = 1, 2, 3$. Our assumptions guarantee the coefficients b_n, indeed the corresponding coefficients for every $k \geq 1$, to be real. Denote by $B(x)$ the sum $\sum_{n \leq x, b_n \neq 0} 1$.

Remark If $N = 1$, then $D = 1$,

$$L_M(s, \mathrm{sym}^1) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and all the coefficients a_n are real.

Theorem 4 *There are positive constants c_4, $d_1 < 1$, d_2, such that $B(x) \geq c_4 x (\log x)^{-d_1}$ moreover*

$$B(x)^{-1} \sum_{n \leq x, b_n < 0} 1 = 1/2 + O\left((\log x)^{-d_2}\right)$$

uniformly for $x \geq 2$.

The positive and negative coefficients b_n are uniformly distributed amongst those that do not vanish.

The arguments being similar, I confine myself to the case of $L(s, \mathrm{sym}^3)$.

The following result of Heilbronn and Landau [5, 6], will be very helpful.

Lemma 3 *Suppose that the Dirichlet series*

$$F(s) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

with $\lambda_1 < \lambda_2 < \cdots$, $\lambda_n \to \infty$, converges for $Re(s) > 1$ and that $a_n \geq 0$. Assume that $F(s) - (s-1)^{-1}$ is regular at $s = 1$. Then

$$\sum_{\lambda_n \leq y} a_n e^{-\lambda_n} = y + O(1).$$

The proof of Theorem 4 requires a number of preliminary results. Consider the restricted Euler product

$$L_M(s, \mathrm{sym}^1) = \prod_{(p, D) = 1} \left(1 - \alpha_p p^{-s}\right)^{-1} \left(1 - \beta_p p^{-s}\right)^{-1}$$

where $\alpha_p + \beta_p$ is real, $\alpha_p\beta_p = 1$. A central issue is the generalised Ramanujan–Petersson conjecture that $|\alpha_p| = |\beta_p| = 1$, c.f. Kim and Shahidi, loc. cit.; but I shall arrange matters to avoid explicit appeal to the size of the individual parameters α_p, β_p.

In what follows q will denote a prime-power, q_0 the prime of which it is a power, $(q_0, D) = 1$.

On the unramified primes define functions $\rho(p^k) = \alpha_p^k + \beta_p^k$, $\psi(p^k) = \alpha_p^{3k} + \alpha_p^k + \beta_p^k + \beta_p^{3k}$, $k = 1, 2, \ldots$. Since the polynomials defining ρ, ψ are symmetric in α_p, β_p, they are also polynomials in $\alpha_p + \beta_p$, $\alpha_p\beta_p$ and, after our assumptions on the coefficients of $L_M(s, \mathrm{sym}^1)$, real. Note that for unramified primes p, $\psi(p)$ is the coefficient of p^{-s} in $L_M(s, \mathrm{sym}^3)$, but $\psi(p^2)$ will not in general be the coefficient of p^{-2s}. Likewise, $\rho(p)$ is the coefficient of p^{-s} in $L_M(s, \mathrm{sym}^1)$, but $\rho(p^2)$ need not be the coefficient of p^{-2s}.

Lemma 4

$$\sum_{q \le x} \rho(q)^8 q^{-1} \log q_0 = 14 \log x + O(1),$$

$$\sum_{q \le x} \psi(q)^2 q^{-1} \log q_0 = \log x + O(1),$$

uniformly for $x \ge 2$.

Proof By direct calculation

$$h(s) = \exp\left(\sum_{p,k,(p,D)=1} \rho(p^k)^8 (kp^{ks})^{-1} \right)$$

$$= L_M(s, \mathrm{sym}^8) L_M(s, \mathrm{sym}^6)^7 L_M(s, \mathrm{sym}^4)^{20} L_M(s, \mathrm{sym}^2)^{28} \zeta_M(s)^{14}.$$

In view of the work of Kim and Shahidi, loc. cit., each of the restricted symmetric product L-functions is analytic in the half-plane $\mathrm{Re}(s) > 1$, analytic and non-zero in a proper disc $|s - 1| < c$; so, therefore, is $h(s)\zeta(s)^{-14}$. For a suitable choice of constant K, $\log\left(Kh(s)\zeta(s)^{-14}\right)$, with principal value of the logarithm, is analytic in a similar region. Differentiating and appealing to standard properties of the Riemann zeta function, we obtain about the points $s = 1$ a Laurent expansion

$$\sum_q \rho(q)^8 q^{-s} \log q_0 = 14(s-1)^{-1} + c_0 + \cdots.$$

Since the coefficients $\rho(q)^8 \log q_0$ are real and non-negative, we may appeal to Lemma 3 with the λ_n running through the $\log q$, to justify the first assertion of Lemma 4.

To justify the second assertion we likewise consider the function

$$\exp\left(\sum_{p,k,(p,D)=1}\psi(p^k)^2(kp^{ks})^{-1}\right)$$
$$= L_M(s,\mathrm{sym}^3\times\mathrm{sym}^3) = L_M(s,\mathrm{sym}^6)L_M(s,\mathrm{sym}^4)L_M(s,\mathrm{sym}^2)\zeta_M(s).$$

Lemma 5 *For a positive constant c and all sufficiently large values of x, the interval* $[2,x]$ *contains at least* $cx/\log x$ *primes on which* $\psi(p)$ *does not vanish.*

Proof Appeal to the second estimate in Lemma 4 and an application of Hölder's inequality shows that

$$\log(x/y)+O(1) = \sum_{y<q\le x}\psi(q)^2q^{-1}\log q_0$$
$$\le\left(\sum_{y<q\le x,\psi(q)\neq0}q^{-1}\log q_0\right)^{1/4}\left(\sum_{y<q\le x}|\psi(q)|^{8/3}q^{-1}\log q_0\right)^{3/4},$$

uniformly for $2\le y\le x$.

By direct calculation $\psi(q) = \rho(q)\left(\rho(q)^2-2\right)$. Moreover, for real x, $\left(x(x^2-2)\right)^2 \le \max(2^5 3^{-3}, x^6)$. The second of the two majorising sums does not exceed

$$\sum_{y<q\le x}\left(\rho(q)^8+2\right)q^{-1}\log q_0$$

which, by the first estimate of Lemma 4, is $16\log(x/y)+O(1)$.

We choose $y=\varepsilon x$ and fix ε at a value sufficiently small that for all large x the first of the two majorising sums exceeds $2^{-13}\log(1/\varepsilon)=\delta>0$. Then

$$\sum_{\varepsilon x<q\le x,\psi(q)\neq0}1\ge\varepsilon\delta x(\log x)^{-1}$$

and the assertion of Lemma 5 follows rapidly.

Lemma 6 *For a positive constant* c_5,

$$\sum_{p\le x,\psi(p)<0}p^{-1}\ge c_5\log\log x+O(1),$$

uniformly for $x\ge2$.

Proof Again appealing to the representation $\psi(q) = \rho(q)\left(\rho(q)^2 - 2\right)$, we see that if $\psi(q)^2 \geq r^6 > 1$, then $|\rho(q)| > r$. Hence

$$\sum_{q\leq x, |\psi(q)|\leq r^6} \psi(q)^2 q^{-1} \log q_0 \geq \sum_{q\leq x} \psi(q)^2 q^{-1} \log q_0 - r^{-2} \sum_{q\leq x} (\rho(q)\psi(q))^2 q^{-1} \log q_0.$$

Moreover, $(\rho(q)\psi(q))^2 \leq \rho(q)^2 \max(2, \rho(q)^6) \leq \max(3, \rho(q)^8)$. Two appeals to Lemma 4 then show that for $r^2 > 17$,

$$\sum_{q\leq x, |\psi(q)|\leq r^6} |\psi(q)| q^{-1} \log q_0 \geq r^{-6}\left(1 - 17r^{-2}\right) \log x + O(1).$$

With $r = 3\sqrt{2}$, $3^8 \cdot 2^4 c_6 = 1$,

$$\sum_{q\leq x} |\psi(q)| q^{-1} \log q_0 \geq c_6 \log x + O(1)$$

and, after an integration by parts,

$$\sum_{p^k\leq x, (p,D)=1} |\psi(p^k)| (kp^k)^{-1} \geq c_6 \log\log x + O(1),$$

uniformly for $x \geq 2$.

Note that, together with an application of the Cauchy–Schwarz inequality, the second estimate of Lemma 4 shows that

$$\sum_{q\leq x} |\psi(q)| q^{-1} \log q_0 \leq \log x + O(1).$$

We shall employ this bound to offset the variability in the sign of $\psi(q)$.

We may modify the argument of Lemma 4, replacing $\psi(q)^2$ by $\psi(q)$, and without differentiation obtain a Laurent expansion

$$\sum_{(p^k,D)=1} \psi(p^k)(kp^{ks})^{-1} = c_7 + \cdots, \quad |s-1| < c.$$

To this end we note that $L_M(s, \mathrm{sym}^3)$ is analytic and non-zero in a proper neighbourhood of $s = 1$. In fact, the existence of a zero of order m at $s = 1$ would require the addition of a term $-m\log(s-1)$ to the sum and increase the value of the constant c_5 in the present lemma.

With $\sigma_0 = 1 + (\log x)^{-1}$, an integration by parts shows

$$(\log x)^{-1} \sum_{q>x} |\psi(q)| q^{-\sigma_0} \log q_0 \quad \text{hence} \quad \sum_{p^k>x, (p,D)=1} |\psi(p^k)| (kp^k)^{-1}$$

to be bounded uniformly for $x \geq 2$. Moreover,

$$\sum_{p^k \leq x,(p,D)=1} |\psi(p^k)|k^{-1}(p^{-k} - p^{-k\sigma_0}) \ll (\log x)^{-1} \sum_{q \leq x} |\psi(q)|q^{-1} \log q_0$$

is also uniformly bounded. So, therefore, is the sum

$$\sum_{p^k \leq x,(p,D)=1} \psi(p^k)(kp^k)^{-1}.$$

Altogether, setting $w(p^k) = k^{-1}$,

$$\begin{aligned} 2S &= 2 \sum_{q \leq x, \psi(p)<0} |\psi(q)|q^{-1}w(q) \\ &\geq \sum_{q \leq x} (|\psi(q)| + \psi(q))\, q^{-1}w(q) \geq c_6 \log\log x + O(1). \end{aligned}$$

The terms with $|\psi(q)| > t > 0$ contribute to S at most $t^{-1} \sum_{q \leq x} |\psi(q)|^2 q^{-1}w(q) \leq t^{-1} \log\log x + O(1)$. For $t > 2c_6^{-1}$,

$$2 \sum_{q \leq x, \psi(q)<0} q^{-1}w(q) \geq (c_6 t^{-1} - 2t^{-2}) \log\log x + O(1).$$

Choosing $tc_6 = 4$,

$$16 \sum_{p \leq x, \psi(p)<0} p^{-1} \geq c_6^2 \log\log x + O(1).$$

Lemma 6 is established.

Proof of Theorem 4 for the Coefficients of $L(s, \mathrm{sym}^3)$ This now rapid. Define the multiplicative function g by assigning to $g(p^k)$ the value $1, -1$ or 0 according to whether b_{p^k} is positive, negative or zero, respectively. That $B(x)$ lies between positive constant multiples of $x(\log x)^{-1} \prod_{p \leq x} \left(1 + |g(p)|p^{-1}\right)$ for $x \geq 2$ follows from Lemmas 5 and 2, the explicit lower bound from a second application of Lemma 5.

That

$$B(x)^{-1} \sum_{n \leq x} g(n) \to 0, \quad x \to \infty,$$

and the negative coefficients b_n are uniformly distributed amongst those that are non-zero follows from Lemma 5, Lemma 6 and Theorem 3.

To gain the sharper estimate of Theorem 4 we give a quantitative aspect to the remark following the statement of Theorem 1.

Let t be a value in the interval $[-(\log x)^4, (\log x)^4]$ for which the sum $\sum_{2<p\le x} p^{-1}(|g(p)| - \operatorname{Re} g(p)p^{it})$ attains its minimum. For z in the complex unit disc $|1-z^2|^2 \le 4|1-z|^2 \le 8(1-\operatorname{Re} z)$. We apply Lemma 1 with $h(p) = |g(p)|$, $z = g(p)p^{it}$, $8\delta^{1/3} = c$. There are two cases.

In the first case the function Λ in the statement of Theorem 1, with $T = (\log x)^4$, satisfies $8\Lambda > \delta \sum_{2<p\le x} p^{-1}$.

In the second case $(c/2)\log\log x \ll 3\theta(4\delta^{-1/3}t) + 3\theta(2t) + 1$. The definition of θ ensures that $|t| \le (\log x)^{-c_8}$ for a positive constant $c_8 < 1$ and all large x. Setting $w = \exp((\log x)^{c_8})$ we note that

$$\sum_{p\le w} p^{-1}|1-p^{it}| \ll |t| \sum_{p\le w} p^{-1}\log p \ll |t|\log w \ll 1.$$

Hence $\Lambda \ge \sum_{p\le w} p^{-1}(|g(p)| - g(p)) + O(1)$, which Lemma 6 shows to exceed $2c_5c_8 \log\log x + O(1)$.

In either case $\Lambda \ge c_9 \log\log x + O(1)$ for a positive c_9 and all $x \ge 2$. Theorem 4 is established.

Remarks For the purposes of establishing uniformity of sign changes in the coefficients b_n, the behaviour of b_{p^k} on powers of finitely many primes is largely irrelevant. It should, perhaps, be emphasised that we do not need an accurate estimate for the number of non-vanishing coefficients b_n; a positive lower density on the primes suffices.

A version of Theorem 4 for $L(s, \mathrm{sym}^1)$ and Maass forms attached to the action of $SL(2,\mathbb{Z})$ on the complex upper half-plane is given in Elliott and Kish [4].

In view of the work of Barnet-Lamb, Geraghty, Harris and Taylor [1], analogues of the sharpened Theorem 4 may be established for symmetric product L-functions, of every order, that are attached to holomorphic forms for the action of a congruence group on the complex upper half-plane, provided the form is not of complex multiplication type. Whilst the error terms in the estimates each save a power of $\log x$, they do not currently have an explicit uniformity in the order of the symmetric product.

An important feature of the present result is the availability of generalisations corresponding to the replacement of the group $GL_2(A_{\mathbb{Q}})$ by $GL_2(A_F)$, with A_F the adèles of a finite algebraic extension, F, of the rationals. With this generality in mind, to establish the present Theorem 4 the argument given in Elliott and Kish [4], needed modification since appropriate analytic properties of the function $\sum_{n=1}^{\infty} \lambda(n)^4 n^{-s}$, effectively of symmetric product L-functions of order 10 and 12, are not currently available.

Concluding Remark The value distribution function

$$F(y) = [x]^{-1} \sum_{n\le x, f(n)\le y} 1, \quad x \ge 1, y \in \mathbb{R},$$

attached to an additive arithmetic function $n \to f(n)$, may be studied through the agency of its Fourier–Stieltjes transform

$$\int_{-\infty}^{\infty} e^{ity} dF(y) = [x]^{-1} \sum_{n \le x} g(n), \quad t \in \mathbb{R},$$

where $n \to g(n) = \exp(itf(n))$ is multiplicative. Multiplicative functions play a central rôle in probabilistic number theory.

The characteristically catholic survey of probabilistic number theory given by Wolfgang in Kanazawa, Japan, 2005 [8], illustrates an aspect of his personality that, quite apart from his mathematics, I shall very much miss: his generosity of spirit.

References

1. T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, A family of Calabi-Yau varieties and potential automorphy II. Publ. Res. Inst. Math. Sci. **47**(1), 29–98 (2011)
2. P.D.T.A. Elliott, *Duality in Analytic Number Theory*. Cambridge Tracts in Mathematics, vol. 122 (Cambridge University Press, Cambridge, 1997)
3. P.D.T.A. Elliott, J. Kish, Harmonic analysis on the positive rationals I: basic results (2014). arXiv:1405.7130
4. P.D.T.A. Elliott, J. Kish, Harmonic analysis on the positive rationals II: multiplicative functions and Maass forms (2014). arXiv:1405.7132
5. H. Heilbronn, E. Landau, Anwendungen der N. Wienerschen Methode. Math. Z. **37**(1), 18–21 (1933); c.f. *The Collected Papers of Hans Arnold Heilbronn*, ed. by E.J. Kari, R.A. Smith. Canadian Mathematical Society Series of Monographs and Advanced Texts (Wiley, New York, 1988)
6. H. Heilbronn, E. Landau, Bemerkungen zur vorstehenden Arbeit von Herrn Bochner. Math. Z. **37**(1), 10–16 (1933); c.f. *The Collected Papers of Hans Arnold Heilbronn*, ed. by E.J. Kari, R.A. Smith. Canadian Mathematical Society Series of Monographs and Advanced Texts (Wiley, New York, 1988)
7. H.H. Kim, F. Shahidi, Cuspidality of symmetric powers with applications. Duke Math. J. **112**(1), 177–197 (2002)
8. W. Schwarz, Some highlights from the history of probabilistic number theory, in *Probability and Number Theory, Proceedings of the International Conference on Probability and Number Theory*, Kanazawa, June 20–24, 2005, ed. by S. Akiyama, K. Matsumoto, L. Murata, H. Sugita. Advanced Studies in Pure Mathematics, vol. 49 (Mathematical Society of Japan, Tokyo, 2007), pp. 367–419
9. W. Schwarz, J. Spilker, *Arithmetical Functions*. London Mathematical Society Lecture Note Series, vol. 184 (Cambridge University Press, Cambridge, 1994)
10. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. II. Acta Math. Acad. Sci. Hung. **18**, 411–467 (1967)

On Error Sum Functions for Approximations with Arithmetic Conditions

Carsten Elsner

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract Let $\mathcal{E}_{k,l}(\alpha) = \sum_{q_m \equiv l \pmod k} |q_m\alpha - p_m|$ be error sum functions formed by convergents p_m/q_m $(m \geq 0)$ of a real number α satisfying the arithmetical condition $q_m \equiv l \pmod k$ with $0 \leq l < k$. The functions $\mathcal{E}_{k,l}$ are Riemann-integrable on $[0, 1]$, so that the integrals $\int_0^1 \mathcal{E}_{k,l}(\alpha)\, d\alpha$ exist as the arithmetical means of the functions $\mathcal{E}_{k,l}$ on $[0, 1]$. We express these integrals by multiple sums on rational terms and prove upper and lower bounds. In the case when l vanishes (i.e. k divides q_m) and when the smallest prime divisor p_1 of $k = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ satisfies $p_1 > k^{\varepsilon}$ for some positive real number ε, we have found an asymptotic expansion in terms of k, namely $\int_0^1 \mathcal{E}_{k,0}(\alpha)\, d\alpha = \zeta(2)\big(2\zeta(3)k^2\big)^{-1} + \mathcal{O}\big(3^t k^{-2-\varepsilon}\big)$. This result includes all integers k which are of the form $k = p^a$ for primes p and integers $a \geq 1$.

Keywords Approximation with arithmetical conditions • Continued fractions • Convergents • Error sum functions

2010 Mathematics subject classification: Primary 11J04; Secondary 11J70

1 Introduction

There are many results in the literature concerned with rational approximations p/q to irrational numbers, where p and q are restricted by additional arithmetical conditions. An important result in this direction is due to Uchiyama [11].

Theorem A *For every real irrational number α and integers $s > 1$, $a \geq 0$, $b \geq 0$ such that a and b are not simultaneously divisible by s, there are infinitely many*

C. Elsner (✉)
Fachhochschule für die Wirtschaft, University of Applied Sciences, Freundallee 15, 30 173 Hannover, Germany
e-mail: carsten.elsner@fhdw.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_9

integers p and $q \neq 0$ satisfying

$$\left|\alpha - \frac{p}{q}\right| < \frac{s^2}{4q^2}, \quad p \equiv a \pmod{s}, \quad q \equiv b \pmod{s}.$$

In [3] the author proved that the constant 1/4 in Uchiyama's paper cannot be improved. Let $\|\eta\|$ denote the distance of a real number η from the nearest integer. Then we deduce the following corollary from Theorem A:

Corollary A1 *Let $f : \mathbb{N} \to \mathbb{R}_{>0}$ be a function satisfying $f(q) = o(q)$ for positive integers q tending to infinity. Then, for every integers $s > 0$, $a \geq 0$ and every real irrational number α we have*

$$\liminf_{\substack{q>0 \\ q \equiv a \pmod{s}}} f(q)\|q\alpha\| = 0.$$

In particular cases stronger results are possible, e.g., for the number $e = \exp(1)$ by Theorem 1.3 in [4].

Theorem B *Let a and s be arbitrary positive integers. Then*

$$\liminf_{\substack{q>0 \\ q \equiv a \pmod{s}}} q\|qe\| = 0.$$

About 5 years later Komatsu [9, Theorem 4] showed that the result of Theorem B remains true for e replaced by every number $e^{1/k}$ ($k \in \mathbb{N}$).

Recently, the author [5] studied the so-called *error sum functions*. Let

$$\mathcal{E}(\alpha) := \sum_{m=0}^{\infty} |q_m\alpha - p_m|, \qquad \mathcal{E}^*(\alpha) := \sum_{m=0}^{\infty} (q_m\alpha - p_m),$$

where for $m \geq 0$ the fraction p_m/q_m is the m-th convergent of the real number α. The numbers p_m and q_m can be computed recursively from the continued fraction expansion of α. Various aspects of these functions have been investigated in [5–7], among them it is shown that $0 \leq \mathcal{E}(\alpha) \leq (1 + \sqrt{5})/2$ and $0 \leq \mathcal{E}^*(\alpha) \leq 1$ for all real numbers α. Both, $\mathcal{E}(\alpha)$ and $\mathcal{E}^*(\alpha)$, measure the average of error terms for diophantine approximations of α by rationals. Moreover, $\mathcal{E}(\alpha) \in \mathbb{Q}(\alpha)$ holds for real numbers of algebraic degree 1 and 2. For $e = \exp(1)$ we have the formula

$$\mathcal{E}(e) = 2e \int_0^1 \exp(-t^2)\, dt - e = 1.3418751\ldots,$$

which proves that $\mathcal{E}(e) \notin \mathbb{Q}(e)$. The function $\mathcal{E}(\alpha)$ is continuous for every real irrational point α, and discontinuous for all rational numbers α (see [6, Theorem 2]).

Therefore, the function $\mathcal{E}$ is Riemann-integrable on $[0, 1]$. It turns out [6, Theorem 5] that

$$\int_0^1 \mathcal{E}(\alpha)\, d\alpha \;=\; -\frac{5}{8} + \frac{3\zeta(2)\log 2}{2\zeta(3)} \;=\; 0.79778798\ldots,$$

where ζ denotes the Riemann Zeta function. This integral represents the arithmetical mean of the function $\mathcal{E}$ on $[0, 1]$. This result can be generalized. Let $n = 1, 2, 3, \ldots$ and

$$I_n \;:=\; \int_0^1 \sum_{m=0}^{\infty} \left|q_m\alpha - p_m\right|^n d\alpha\,.$$

It can be shown [6, Sec. 4] that

$$I_n \;=\; \frac{1}{n+1}\left(1 - \frac{1}{2^{n+1}} - \frac{2\zeta(n+1,-1)}{\zeta(n+2)}\right),$$

where

$$\zeta(n+1,-1) \;:=\; \sum_{m_2>m_1>0} \frac{(-1)^{m_1}}{m_1 m_2^{n+1}} \;=\; \sum_{m_2=1}^{\infty} \frac{1}{m_2^{n+1}} \sum_{m_1=1}^{m_2-1} \frac{(-1)^{m_1}}{m_1}$$

is known as multiple Zeta function. Borwein et al. [2] expressed $\zeta(n+1,-1)$ in terms of $\log 2, \zeta(2), \zeta(3), \ldots, \zeta(n+2)$. Thus we obtain the following results:

Theorem C *Let $n \geq 1$ be an integer. Then we have*

$$\int_0^1 \sum_{m=0}^{\infty} \left|q_m\alpha - p_m\right|^n d\alpha \;=\; \frac{1}{n+1}\left(1 - \frac{1}{2^{n+1}}\right) - 1 + \frac{4\log(2)\,\zeta(n+1)}{(n+1)\zeta(n+2)}\left(1 - \frac{1}{2^{n+1}}\right)$$
$$+ \frac{1}{(n+1)\zeta(n+2)} \sum_{k=1}^{n-1} \left(1 - \frac{1}{2^k}\right)\left(1 - \frac{1}{2^{n-k}}\right)\zeta(k+1)\zeta(n+1-k)\,.$$

In particular, for $n = 2, 3, 4$ we have the identities

$$\int_0^1 \sum_{m=0}^{\infty} \left|q_m\alpha - p_m\right|^2 d\alpha \;=\; \frac{7\log 2\,\zeta(3)}{6\zeta(4)} + \frac{\zeta^2(2)}{12\zeta(4)} - \frac{17}{24} \;=\; 0,39813\ldots,$$

$$\int_0^1 \sum_{m=0}^{\infty} \left|q_m\alpha - p_m\right|^3 d\alpha \;=\; \frac{15\log 2\,\zeta(4)}{16\zeta(5)} + \frac{3\zeta(2)\zeta(3)}{16\zeta(5)} - \frac{49}{64} \;=\; 0,27019\ldots,$$

$$\int_0^1 \sum_{m=0}^{\infty} \left|q_m\alpha - p_m\right|^4 d\alpha \;=\; \frac{31\log 2\,\zeta(5)}{40\zeta(6)} + \frac{7\zeta(2)\zeta(4)}{40\zeta(6)} + \frac{9\zeta^2(3)}{80\zeta(6)} - \frac{129}{160} \;=\; 0,20731\ldots.$$

Taking $\zeta(2s) \in \mathbb{Q}(\pi)$ into account, it follows that

$$\begin{aligned}
I_1 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3)\big)\,,\\
I_2 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3)\big)\,,\\
I_3 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3), \zeta(5)\big)\,,\\
I_4 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3), \zeta(5)\big)\,,\\
I_5 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3), \zeta(5), \zeta(7)\big)\,,\\
I_6 &\in \mathbb{Q}\big(\pi, \log(2), \zeta(3), \zeta(5), \zeta(7)\big)\,;
\end{aligned}$$

in particular we know $I_1, \ldots, I_6 \in \mathbb{Q}\big(\pi, \log(2), \zeta(3), \zeta(5), \zeta(7)\big)$. This proves that $I_1, \ldots, I_6$ are algebraically dependent over $\mathbb{Q}$. But indeed a stronger result holds, which can be verified using a suitable computer algebra system.

Corollary C1 *The numbers I_1, I_2, I_3, I_4 are algebraically dependent over $\mathbb{Q}$. For $x_i = I_i$ $(i = 1, 2, 3, 4)$ the algebraic equation*

$$\begin{aligned}
0 = {} & 10240x_1x_3x_4 - 2976x_1^2x_2 - 1488x_1^2 - 5952x_1x_2 + 5120x_1x_3 + 7840x_1x_4\\
& -2592x_2x_3 + 6400x_3x_4 + 944x_1 - 4542x_2 + 1904x_3 + 4900x_4 + 179
\end{aligned}$$

holds.

The proof works by substituting the above expressions for I_1, I_2, I_3, I_4 into the equation given in the corollary, where additionally

$$\zeta(2) = \frac{\pi^2}{6}\,, \qquad \zeta(4) = \frac{\pi^4}{90}\,, \qquad \zeta(6) = \frac{\pi^6}{945}$$

must be taken into account.

Note that

$$I_1, \ldots, I_{2n} \in \mathbb{Q}\big(\underbrace{\pi, \log(2), \zeta(3), \zeta(5), \ldots, \zeta(2n+1)}_{n+2}\big)\,.$$

This proves

Corollary C2 *For every integer $n \geq 3$ any $n+3$ numbers from the set $\{I_1, I_2, \ldots I_{2n}\}$ are algebraically dependent over $\mathbb{Q}$.*

In this paper we focus our interest on a generalized error sum function. Let α be a real number, and let $k \geq 1$ and $0 \leq l < k$ be integers. We define

$$\mathcal{E}_{k,l}(\alpha) := \sum_{\substack{m=0\\ q_m \equiv l \pmod k}}^{\infty} |q_m\alpha - p_m|\,,$$

in particular we set $\mathcal{E}_k(\alpha) = \mathcal{E}_{k,0}(\alpha)$. It is clear that $\mathcal{E}_1(\alpha) = \mathcal{E}(\alpha)$, and

$$\sum_{l=0}^{k-1} \mathcal{E}_{k,l}(\alpha) \;=\; \mathcal{E}(\alpha) \qquad (k \geq 1)\,.$$

For $k > 1$ the error sum function $\mathcal{E}_k(\alpha)$ can be transformed into a more striking form. Since k does not divide $q_0 = 1$, the term for $m = 0$ in $\mathcal{E}_k(\alpha)$ does not occur. Moreover, for the convergents p_m/q_m $(m \geq 1)$ of α satisfying $q_m \equiv 0 \pmod{k}$ we obtain the inequalities

$$|q_m\alpha - p_m| \;\leq\; \frac{1}{q_m} \;\leq\; \frac{1}{k} \;\leq\; \frac{1}{2}\,.$$

This proves

$$\mathcal{E}_k(\alpha) \;=\; \sum_{\substack{m=1 \\ k|q_m}}^{\infty} \|q_m\alpha\| \qquad (k > 1)\,. \tag{1.1}$$

We continue to point out more basic properties of $\mathcal{E}_k(\alpha)$ for $k > 1$. Since q_m and q_{m+1} are coprime, at most every second term in $\mathcal{E}_k(\alpha)$ does not vanish. So we obtain the following upper bound for $\mathcal{E}_k(\alpha)$:

$$\mathcal{E}_k(\alpha) \;=\; \sum_{\substack{m=1 \\ k|q_m}}^{\infty} |q_m\alpha - p_m| \;\leq\; \sum_{m=0}^{\infty} |q_{2m+1}\alpha - p_{2m+1}| \;=\; \frac{\mathcal{E}(\alpha) - \mathcal{E}^*(\alpha)}{2} \qquad (k > 1)\,.$$

The identities

$$\mathcal{E}_k(\alpha) \;=\; \frac{\mathcal{E}(\alpha) - \mathcal{E}^*(\alpha)}{2} \;=\; \alpha$$

with $k > 1$ hold for all numbers α given by their continued fraction expansion

$$\alpha \;=\; [0; k, 1, k, 1, k, 1, \ldots] \;=\; [0; \overline{k, 1}] \;=\; \sqrt{\frac{1}{4} + \frac{1}{k}} - \frac{1}{2}\,,$$

since for $m \geq 0$ we have the congruence relations $q_{2m+1} \equiv 0 \pmod{k}$ and $q_{2m} \equiv 1 \pmod{k}$. Moreover,

$$\mathcal{E}_k(\alpha) \;=\; \sum_{m=0}^{\infty} |q_{2m+1}\alpha - p_{2m+1}| \;=\; \sum_{m=0}^{\infty} \left(\frac{k+2}{2} - \sqrt{\Big(\frac{k+2}{2}\Big)^2 - 1} \right)^{m+1} \;=\; \alpha\,.$$

There exist real irrational numbers α for which the series $\mathcal{E}_k(\alpha)$ consists of at most finitely many terms, contrary to the series $\mathcal{E}(\alpha)$. To prove the existence of such an irrational number, we define α recursively by its continued fraction expansion $\alpha = [0; a_1, a_2, \dots] = [0; 2, 1, 1, 2, 2, 4, 6, \dots]$ as follows. We have

$$q_1 = 2\,, \quad q_2 = 3\,, \quad q_3 = 5\,, \quad q_4 = 13\,, \quad q_5 = 31\,, \quad q_6 = 137\,, \quad q_7 = 853\,.$$

Now let us assume that for $m \geq 8$ the denominators q_{m-1} and q_{m-2} are primes. Then, by the Dirichlet prime number theorem, there are infinitely many positive integers a such that $q_m = aq_{m-1} + q_{m-2} \in \mathbb{P}$. The number a_m is uniquely defined by the smallest positive integer a satisfying this condition. Then, for *every* integer $k > 1$, the series $\mathcal{E}_k(\alpha)$ consists of at most one term. Furthermore, there are many situations in which $\mathcal{E}_k(\alpha)$ vanishes.

Proposition 1.1 *For every integer $k > 1$ there are uncountably many irrational numbers α such that $\mathcal{E}_k(\alpha) = 0$.*

To prove this proposition, let $k > 1$ be any integer. We define an irrational number α depending on k and on a sequence $(b_n)_{n\geq 2}$ of positive integers by

$$\alpha = [0; 1, kb_2, kb_3, kb_4, \dots] = [0; a_1, a_2, a_3, \dots]\,.$$

The denominators q_m of the convergents p_m/q_m of α satisfy the recurrence formula

$$q_0 = 1\,, \quad q_1 = a_1 = 1\,, \quad q_{m+2} = a_{m+2}q_{m+1} + q_m \quad (m = 0, 1, 2, \dots)\,.$$

Since $q_{m+2} \equiv q_m \pmod{k}$ for $m = 0, 1, 2, \dots$ it follows recursively that $1 \equiv q_0 \equiv q_2 \equiv q_4 \equiv \cdots \equiv q_{2m} \pmod{k}$ and, similarly, $1 \equiv q_1 \equiv q_3 \equiv q_5 \equiv \cdots \equiv q_{2m+1} \pmod{k}$ for $m = 0, 1, 2, \dots$. This proves that no denominator q_m is divisible by k. Hence, $\mathcal{E}_k(\alpha) = 0$. By Cantor's counting principle we have found uncountably many real numbers α satisfying $\mathcal{E}_k(\alpha) = 0$.

The main goal of this paper is to study the behaviour of the numbers $\int_0^1 \mathcal{E}_{k,l}(\alpha)\, d\alpha$ depending on k and l. For $l = 0$ and k restricted to those numbers having *no small prime divisors* we prove the asymptotic behaviour of these integrals for k tending to infinity (Theorem 2.1 and Corollaries 2.2–2.5). For integers k having *many small prime divisors* the numbers $\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha$ tend more quickly to zero than in the case $k = p^a$ for fixed $a \geq 1$ and primes p (Theorem 2.6 and Corollary 2.4). The integrals on the error sum functions $\mathcal{E}_{k,l}$ with $l > 0$ are treated in Theorem 2.7.

2 Statement of the Results

Let $\mu : \mathbb{N} \to \{-1, 0, 1\}$ be the Möbius function, and let $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ for $s \geq 2$ be the Riemann Zeta function. By $J_3 : \mathbb{N} \to \mathbb{N}$ we denote Jordan's arithmetical function defined by $J_3(1) = 1$ and

$$J_3(n) \;=\; n^3 \prod_{p|n} \Big(1 - \frac{1}{p^3}\Big) \qquad (n > 1)\,, \tag{2.1}$$

where p runs through all prime divisors of n. Moreover, for any integer n let $\mathcal{D}_n$ denote the set of all positive divisors of n. For every positive integer r we define the number T_r by

$$T_r \;:=\; \sum_{n=r}^{\infty} \sum_{1 \leq m \leq n/r} \frac{(-1)^{m+1}}{mn^2}\,. \tag{2.2}$$

The identity from the following theorem can be considered as the main result of this paper, which contrasts with the property of the function $\mathcal{E}_k(\alpha)$ given by Proposition 1.1.

Theorem 2.1 *For every integer $k > 1$ we have*

$$\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha \;=\; \frac{1}{\zeta(3)} \sum_{r \in \mathcal{D}_k} \sum_{s \in \mathcal{D}_r} \frac{\mu(s)\mu(ks/r)T_r}{rJ_3(ks/r)}\,.$$

Corollary 2.2 *Let $k > 1$ be any integer having t prime divisors , where P denotes the smallest prime divisor of k. Then we have*

$$\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha \;=\; \frac{\zeta(2)}{2\zeta(3)k^2} + \mathcal{O}\Big(\frac{1}{k^3} + \frac{3^t}{k^2 P}\Big)\,.$$

Corollary 2.3 *For all primes p we have*

$$\int_0^1 \mathcal{E}_p(\alpha)\, d\alpha \;=\; \frac{1}{p^3 - 1}\Big(\frac{p^2 T_p}{\zeta(3)} - \frac{3\zeta(2)\log 2}{2\zeta(3)} + \frac{1}{4}\Big) \;=\; \frac{\zeta(2)}{2\zeta(3)p^2} + \mathcal{O}\Big(\frac{1}{p^3}\Big)$$

and

$$\frac{2}{77p^2} \;<\; \int_0^1 \mathcal{E}_p(\alpha)\, d\alpha \;<\; \frac{97}{109p^2} \qquad (p \geq 3)\,.$$

Corollary 2.4 *Let p be a prime and a be a positive integer. Set $k := p^a$. Then we have*

$$\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \;=\; \frac{\zeta(2)}{2\zeta(3)k^2} + \mathcal{O}\Big(\frac{1}{k^{2+1/a}}\Big).$$

Corollary 2.5 *Let $k > 1$ be an integer having at most t prime divisors. The smallest prime divisor P of k satisfies $P > k^{\varepsilon}$ for any $0 < \varepsilon < 1$. Then we have*

$$\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \;=\; \frac{\zeta(2)}{2\zeta(3)k^2} + \mathcal{O}\Big(\frac{3^t}{k^{2+\varepsilon}}\Big).$$

To state the results in the subsequent theorems we need Euler's totient φ.

Theorem 2.6 *For every integer $k \geq 3$ we have*

$$\frac{1}{k^2\log\log k} \;\ll\; \frac{\varphi(k)}{4k^3} \;<\; \int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \;<\; \frac{\zeta(2)}{k^2}.$$

For the numbers $k = p_1p_2\cdots p_r$ given by the product on the first $r \geq 2$ primes $p_1 = 2, p_2 = 3, \ldots$ we have

$$\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \;\asymp\; \frac{1}{k^2\log\log k}.$$

Theorem 2.6 shows that $\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \asymp k^{-2}$ does not hold for $k \in \mathbb{N}$ tending to infinity. In the following theorem we estimate the integral on the error sum function $\mathcal{E}_{k,l}(\alpha)$ for $l > 0$, where the case $l = 1$ is treated separately. By (a, b) we denote the greatest common divisor of two integers a and b.

Theorem 2.7 (i) *For every integer $k \geq 2$ and $l = 1$ we have*

$$\frac{5}{8} + \frac{\varphi(k+1)}{4(k+1)^3} < \int_0^1 \mathcal{E}_{k,1}(\alpha)\,d\alpha = \sum_{\substack{a=1\\ a\equiv 1 \pmod k}}^{\infty} \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} - \frac{3}{8} \leq \frac{5}{8} + \frac{\zeta(2)}{k^2}.$$

(ii) *For integers $k \geq 3$ and $2 \leq l < k$ we have*

$$\frac{\varphi(l)}{4l^3} < \int_0^1 \mathcal{E}_{k,l}(\alpha)\,d\alpha = \sum_{\substack{a=1\\ a\equiv l \pmod k}}^{\infty} \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} \leq \frac{1}{l^2} + \frac{\zeta(2)}{k^2}.$$

For two consecutive primes p_{r-1} and p_r ($r \geq 2$) it follows from *(ii)* in Theorem 2.7 by Bertrand's Postulate and Theorem 9 in [8] that

$$\int_0^1 \mathcal{E}_{p_r,p_{r-1}}(\alpha)\, d\alpha \asymp \frac{1}{p_r^2} \asymp \frac{1}{r^2 \log^2 r}.$$

3 Auxiliary Results

Lemma 3.1 *Let $k > 1$ be an integer, and let r be any positive divisor of k. Then we have the identity*

$$\sum_{\substack{d=1 \\ (d,k)=k/r}}^{\infty} \frac{\mu(d)}{d^3} = \frac{1}{\zeta(3)} \sum_{s \in \mathcal{D}_r} \frac{\mu(s)\mu(ks/r)}{J_3(ks/r)}.$$

Proof We obtain

$$S := \sum_{\substack{d=1 \\ (d,k)=k/r}}^{\infty} \frac{\mu(d)}{d^3} = \sum_{\substack{m=1 \\ (m,r)=1}}^{\infty} \frac{\mu(mk/r)}{(mk/r)^3} = \left(\frac{r}{k}\right)^3 \sum_{m=1}^{\infty} \sum_{\substack{s \geq 1 \\ s|(m,r)}} \frac{\mu(s)\mu(mk/r)}{m^3}$$

$$= \left(\frac{r}{k}\right)^3 \sum_{\substack{s \geq 1 \\ s|r}} \mu(s) \sum_{\substack{m=1 \\ m \equiv 0 \pmod{s}}}^{\infty} \frac{\mu(mk/r)}{m^3} = \left(\frac{r}{k}\right)^3 \sum_{s \in \mathcal{D}_r} \frac{\mu(s)}{s^3} \sum_{m=1}^{\infty} \frac{\mu(mks/r)}{m^3}.$$

For any positive integer t we have

$$\sum_{m=1}^{\infty} \frac{\mu(mt)}{m^3} = \mu(t) \sum_{\substack{m=1 \\ (m,t)=1}}^{\infty} \frac{\mu(m)}{m^3} = \frac{\mu(t)t^3}{\zeta(3)J_3(t)},$$

where the identity on the right-hand side can be obtained by using the method explained in [10]. Substituting the last expression into S by setting $t = ks/r$, we complete the proof of the desired identity from the lemma. □

Lemma 3.2 *For every positive integer r we have*

$$T_r = \sum_{n=1}^{\infty}\sum_{m=0}^{nr-1}\frac{1}{n(nr+m)^2}, \qquad T_1 = \frac{3}{2}\zeta(2)\log 2 - \frac{1}{4}\zeta(3),$$

$$T_r = \frac{\zeta(2)}{2r} + \mathcal{O}\Big(\frac{1}{r^2}\Big), \qquad \text{and} \qquad \frac{1}{2r} < T_r < \begin{cases} \dfrac{1}{r-1} & \text{if } r \geq 2, \\ 1 & \text{if } r \geq 1. \end{cases}$$

In particular, we have $T_r < 2/r$ for all $r \geq 1$.

Proof Let $r \geq 1$ be an integer. To prove the alternative expression of T_r, we first observe that

$$\sum_{n=1}^{\infty}\sum_{m=0}^{nr-1}\frac{1}{n(nr+m)^2} = \sum_{n=1}^{\infty}\frac{1}{n}\sum_{k=nr}^{2nr-1}\frac{1}{k^2} = \sum_{k=r}^{\infty}\frac{1}{k^2}\sum_{n=\lfloor k/2r\rfloor+1}^{\lfloor k/r\rfloor}\frac{1}{n}, \tag{3.1}$$

where the last identity follows by interchanging the order of summation, and where $\lfloor\eta\rfloor$ denotes the floor function, i.e. the greatest integer not exceeding η. Next, let $\beta \geq 1$ be a real number, and

$$\delta := \begin{cases} 1, \text{ if } \lfloor\beta\rfloor \equiv 1 \pmod 2, \\ 0, \text{ if } \lfloor\beta\rfloor \equiv 0 \pmod 2. \end{cases}$$

Then we have

$$\sum_{n=1}^{\lfloor\beta\rfloor}\frac{1}{n} = \sum_{m=1}^{\lfloor\beta/2\rfloor+\delta}\frac{1}{2m-1} + \sum_{m=1}^{\lfloor\beta/2\rfloor}\frac{1}{2m},$$

which yields, equivalently,

$$\begin{aligned}\sum_{n=\lfloor\beta/2\rfloor+1}^{\lfloor\beta\rfloor}\frac{1}{n} &= \sum_{m=1}^{\lfloor\beta/2\rfloor+\delta}\frac{1}{2m-1} + \frac{1}{2}\sum_{m=1}^{\lfloor\beta/2\rfloor}\frac{1}{m} - \sum_{n=1}^{\lfloor\beta/2\rfloor}\frac{1}{n} \\ &= \sum_{m=1}^{\lfloor\beta/2\rfloor+\delta}\frac{1}{2m-1} - \frac{1}{2}\sum_{m=1}^{\lfloor\beta/2\rfloor}\frac{1}{m} \\ &= \sum_{m=1}^{\lfloor\beta\rfloor}\frac{(-1)^{m+1}}{m}.\end{aligned}$$

With $\beta = k/r$ for $k \geq r$ we conclude from (3.1) and (2.2) that

$$\sum_{n=1}^{\infty} \sum_{m=0}^{nr-1} \frac{1}{n(nr+m)^2} = \sum_{k=r}^{\infty} \frac{1}{k^2} \sum_{1 \leq m \leq k/r} \frac{(-1)^{m+1}}{m} = T_r \,.$$

For the asymptotic expansion of T_r we apply Euler's summation formula to the function $f(x) = 1/(x+nr-1)^2$: Let $B(\eta) = \eta - [\eta] - 1/2$. Then,

$$\begin{aligned} \sum_{m=1}^{nr} \frac{1}{(x+nr-1)^2} &= \int_1^{nr} f(x)\,dx + \int_1^{nr} B(x) f'(x)\,dx - B(1)f(1) - B(nr)f(nr) \\ &= \frac{1}{nr} - \frac{1}{2nr-1} + \mathcal{O}\Big(\frac{1}{n^2 r^2}\Big)\,, \end{aligned}$$

which yields

$$\begin{aligned} T_r &= \sum_{n=1}^{\infty} \frac{1}{n} \sum_{m=1}^{nr} \frac{1}{(x+nr-1)^2} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^2 r} - \sum_{n=1}^{\infty} \frac{1}{n(2nr-1)} + \mathcal{O}\Big(\sum_{n=1}^{\infty} \frac{1}{n^3 r^2}\Big) \\ &= \frac{\zeta(2)}{r} - \sum_{n=1}^{\infty} \Big(\frac{1}{2n^2 r} + \frac{1}{2n^2 r(2nr-1)}\Big) + \mathcal{O}\Big(\frac{1}{r^2}\Big) \\ &= \frac{\zeta(2)}{r} - \frac{\zeta(2)}{2r} + \mathcal{O}\Big(\sum_{n=1}^{\infty} \frac{1}{n^2 r(2nr-1)}\Big) + \mathcal{O}\Big(\frac{1}{r^2}\Big) \\ &= \frac{\zeta(2)}{2r} + \mathcal{O}\Big(\frac{1}{r^2}\Big)\,. \end{aligned}$$

T_1 is a special case of the multivariate zeta function $\zeta(m,n)$, see [1, Sect. 2.6]:

$$\begin{aligned} T_1 &= \sum_{n=1}^{\infty} \sum_{m=1}^{n} \frac{(-1)^{m+1}}{mn^2} = \sum_{n=1}^{\infty} \sum_{m=1}^{n-1} \frac{(-1)^{m+1}}{mn^2} + \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^3} \\ &= -\zeta(2,-1) + \frac{3}{4}\zeta(3) = \frac{3}{2}\zeta(2)\log 2 - \frac{1}{4}\zeta(3)\,. \end{aligned}$$

The bounds for T_r stated in the lemma follow from (2.2) by using the inequalities

$$\frac{1}{2} \le \sum_{1\le m\le n/r} \frac{(-1)^{m+1}}{m} \le 1 \qquad (n \ge r)\,,$$

$$\sum_{m=r}^{\infty} \frac{1}{m^2} < \int_{r-1}^{\infty} \frac{dt}{t^2} = \frac{1}{r-1} \le \frac{2}{r} \quad (r \ge 2)\,, \qquad T_1 = 1.409757\cdots < 2\,,$$

and

$$\sum_{m=r}^{\infty} \frac{1}{m^2} > \int_{r}^{\infty} \frac{dt}{t^2} = \frac{1}{r} \quad (r \ge 1)\,.$$

4 Proof of Theorem 2.1

Let $\chi_{k,l} : \mathbb{N} \to \{0, 1\}$ be defined by

$$\chi_{k,l}(n) := \begin{cases} 1 \text{ if } n \equiv l \pmod{k}\,, \\ 0 \text{ otherwise}\,. \end{cases}$$

Note that $\chi_{k,l}(1) = 1$ holds if and only if $l = 1$. At the beginning of the proof of Theorem 2.1 we follow the lines in Sect. 4 in [6] and modify the arguments. Let m and $a_1, \ldots, a_m$ be positive integers. We define the rational numbers ξ_1, ξ_2 by their continued fraction expansion:

$$\xi_1 = [0; a_1, \ldots, a_{m-1}, a_m] \qquad \text{and} \qquad \xi_2 = [0; a_1, \ldots, a_{m-1}, a_m + 1]\,.$$

We have $\xi_1 < \xi_2$ for even m and $\xi_2 < \xi_1$ for odd m. We define the interval I_m by $I_m = (\xi_1, \xi_2)$ for even m and $I_m = (\xi_2, \xi_1)$ otherwise. It is well known that the intervals I_m are disjoint for different positive integers $a_1, \ldots, a_m$, and that for any fixed m the union of all closed intervals $\overline{I}_m$ gives the interval $[0, 1]$. For this decomposition of $[0, 1]$ we express the integral as follows:

$$\begin{aligned}
\int_0^1 \mathcal{E}_{k,l}(\alpha)\, d\alpha &= \int_0^1 \sum_{m=0}^{\infty} (-1)^m \chi_{k,l}(q_m)(q_m\alpha - p_m)\, d\alpha \\
&= \frac{\chi_{k,l}(1)}{2} + \sum_{m=1}^{\infty} (-1)^m \int_0^1 \chi_{k,l}(q_m)(q_m\alpha - p_m)\, d\alpha \\
&= \frac{\chi_{k,l}(1)}{2} + \sum_{m=1}^{\infty} (-1)^m \sum_{a_1=1}^{\infty} \cdots \sum_{a_m=1}^{\infty} \int_{I_m} \chi_{k,l}(q_m)(q_m\alpha - p_m)\, d\alpha \\
&= \frac{\chi_{k,l}(1)}{2} + \sum_{m=1}^{\infty} \sum_{a_1=1}^{\infty} \cdots \sum_{a_m=1}^{\infty} \chi_{k,l}(q_m) \int_{\xi_1}^{\xi_2} (q_m\alpha - p_m)\, d\alpha\,.
\end{aligned}$$

Note that p_m and q_m depend on $a_1, \dots, a_m$. The continued fraction expansion of every point $\alpha \in I_m$ has the form $\alpha = [0; a_1, \dots, a_{m-1}, a_m, \dots]$. Hence the convergents p_ν/q_ν for $\nu \le m$ depend on I_m, but not on $\alpha \in I_m$. Therefore we compute the above integral on $[\xi_1, \xi_2]$ by

$$\int_{\xi_1}^{\xi_2} (q_m\alpha - p_m)\, d\alpha = (\xi_2 - \xi_1)\, \frac{(\xi_2 + \xi_1)q_m - 2p_m}{2}\,.$$

Using

$$\xi_1 = \frac{p_m}{q_m} \quad \text{and} \quad \xi_2 = \frac{(a_m + 1)p_{m-1} + p_{m-2}}{(a_m + 1)q_{m-1} + q_{m-2}}$$

we compute the expressions

$$\xi_2 - \xi_1 = \frac{(-1)^m}{(q_m + q_{m-1})q_m}$$

and

$$\xi_2 + \xi_1 = \frac{p_{m-1}q_m + q_{m-1}p_m + 2p_m q_m}{(q_m + q_{m-1})q_m}\,,$$

which give

$$\int_{\xi_1}^{\xi_2} (q_m\alpha - p_m)\, d\alpha = \frac{1}{2q_m(q_m + q_{m-1})^2}\,,$$

and consequently

$$\int_0^1 \mathcal{E}_{k,l}(\alpha)\, d\alpha \;=\; \frac{\chi_{k,l}(1)}{2} + \sum_{m=1}^{\infty} \sum_{a_1=1}^{\infty} \cdots \sum_{a_m=1}^{\infty} \frac{\chi_{k,l}(q_m)}{2q_m(q_m + q_{m-1})^2}\,. \tag{4.1}$$

For the denominators of two subsequent convergents of the continued fraction of $\alpha = \langle 0; a_1, \dots, a_m, \dots \rangle$ it is well known that $(q_m, q_{m-1}) = 1$. For fixed $q_m = a$ we count the solutions of $q_{m-1} = b$ with $(a, b) = 1$ and $0 \le b \le a - 1$ in the multiple sum on the left-hand side of (4.1). It is necessary to distinguish the cases $m \ge 2$ and $m = 1$.

Case 1: $m \ge 2$. First let $a_1 = 1$. Then,

$$\frac{q_{m-1}}{q_m} = \langle 0; a_m, \dots, a_2, 1 \rangle = \langle 0; a_m, \dots, a_2 + 1 \rangle\,.$$

For $a_1 \geq 2$ we have

$$\frac{q_{m-1}}{q_m} = \langle 0; a_m, \ldots, a_2, a_1 \rangle = \langle 0; a_m, \ldots, a_2, a_1 - 1, 1 \rangle .$$

Case 2: $m = 1$. For $a_1 = 1$ we have a unique representation of the fraction

$$\frac{q_{m-1}}{q_m} = \frac{q_0}{q_1} = \frac{1}{a_1} = \frac{1}{1} = \langle 0; 1 \rangle ,$$

since the integer part $a_0 = 0$ must not be changed. For $a_1 \geq 2$ there are again two representations:

$$\frac{q_{m-1}}{q_m} = \frac{q_0}{q_1} = \frac{1}{a_1} = \langle 0; a_1 \rangle = \langle 0; a_1 - 1, 1 \rangle .$$

Therefore it becomes clear that for any fixed $q_m = a$ every coprime integer b with $0 \leq b \leq a - 1$ occurs exactly two times in the multiple sum on the right-hand side of (4.1), except for $m = 1$ and $a_1 = 1$. For this exceptional case we separate the term

$$\frac{\chi_{k,l}(q_1)}{2q_1(q_1 + q_0)^2} = \frac{\chi_{k,l}(1)}{8}$$

from the multiple sum. Therefore we obtain

$$\begin{aligned}
&\int_0^1 \mathcal{E}_{k,l}(\alpha)\, d\alpha \\
&= \frac{\chi_{k,l}(1)}{2} + \sum_{m=2}^{\infty} \sum_{a_1=1}^{\infty} \cdots \sum_{a_m=1}^{\infty} \frac{\chi_{k,l}(q_m)}{2q_m(q_m + q_{m-1})^2} + \sum_{a_1=2}^{\infty} \frac{\chi_{k,l}(q_1)}{2q_1(q_1+1)^2} + \frac{\chi_{k,l}(1)}{8} \\
&= \frac{5\chi_{k,l}(1)}{8} + \sum_{a=1}^{\infty} \sum_{\substack{b=1 \\ (a,b)=1}}^{a-1} \frac{\chi_{k,l}(a)}{a(a+b)^2} \\
&= -\frac{3\chi_{k,l}(1)}{8} + \sum_{\substack{a=1 \\ a \equiv l \pmod k}}^{\infty} \sum_{\substack{b=0 \\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} . \qquad (4.2)
\end{aligned}$$

Note that for $b = 0$ the condition $(a, 0) = 1$ holds for $a = 1$ only. For the proof of Theorem 2.1 we now assume that $l = 0$, so that $\chi_{k,l}(1)$ vanishes. Then (4.2) simplifies to

$$\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha \;=\; \sum_{\substack{a=1\\ k|a}}^{\infty} \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2}\,. \tag{4.3}$$

Next, we express the arithmetic condition $(a, b) = 1$ on a and b from the inner sum by the Möbius function. Then we proceed by interchanging the order of the resulting triple sum. Here, $[d, k]$ denotes the least common multiple of d and k.

$$\begin{aligned}\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha \;&=\; \sum_{\substack{a=1\\ k|a}}^{\infty} \sum_{b=0}^{a-1} \sum_{\substack{d>0\\ d|(a,b)}} \frac{\mu(d)}{a(a+b)^2} \;=\; \sum_{d=1}^{\infty} \sum_{\substack{a=1\\ [d,k]\,|\,a}}^{\infty} \sum_{\substack{b=0\\ d|b}}^{a-1} \frac{\mu(d)}{a(a+b)^2}\\ &=\; \sum_{d=1}^{\infty}\sum_{n=1}^{\infty} \sum_{m=0}^{([d,k]n-1)/d} \frac{\mu(d)}{[d,k]n\big([d,k]n+dm\big)^2}\\ &=\; \sum_{r\in\mathcal{D}_k} \sum_{\substack{d=1\\ (d,k)=k/r}}^{\infty} \sum_{n=1}^{\infty} \sum_{m=0}^{[d,k]n/d-1} \frac{\mu(d)}{[d,k]n\big([d,k]n+dm\big)^2}.\end{aligned}$$

The condition $(d, k) = k/r$ implies that

$$[d, k] \;=\; \frac{dk}{(d,k)} \;=\; dr\,.$$

Hence the above multiple sum takes the form

$$\begin{aligned}\int_0^1 \mathcal{E}_k(\alpha)\, d\alpha \;&=\; \sum_{r\in\mathcal{D}_k} \sum_{\substack{d=1\\ (d,k)=k/r}}^{\infty} \sum_{n=1}^{\infty}\sum_{m=0}^{nr-1} \frac{\mu(d)}{nrd(nrd+md)^2}\\ &=\; \sum_{r\in\mathcal{D}_k} \frac{1}{r}\Big(\sum_{\substack{d=1\\ (d,k)=k/r}}^{\infty} \frac{\mu(d)}{d^3}\Big)\Big(\sum_{n=1}^{\infty}\sum_{m=0}^{nr-1} \frac{1}{n(nr+m)^2}\Big)\,.\end{aligned}$$

Finally, we express the two terms in brackets by the identities given in Lemma 3.1 and Lemma 3.2, respectively. This completes the proof of the theorem. □

5 Proofs of Corollaries 2.2–2.5

Proof of Corollary 2.2 From the multiple sum in Theorem 2.1 we separate the term for $r = k$ and $s = 1$:

$$\begin{aligned}\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha &= \frac{T_k}{\zeta(3)k} + \frac{1}{\zeta(3)} \sum_{\substack{r \in \mathcal{D}_k \\ r \neq k \vee s \neq 1}} \sum_{s \in \mathcal{D}_r} \frac{\mu(s)\mu(ks/r)T_r}{rJ_3(ks/r)} \\ &= \frac{T_k}{\zeta(3)k} + \mathcal{O}\Big(\sum_{\substack{r \in \mathcal{D}_k \\ r \neq k \vee s \neq 1}} \sum_{s \in \mathcal{D}_r} \frac{|\mu(s)\mu(ks/r)|T_r}{rJ_3(ks/r)} \Big) \\ &= \frac{T_k}{\zeta(3)k} + \mathcal{O}\Big(\sum_{\substack{r \in \mathcal{D}_k \\ r \neq k \vee s \neq 1}} \sum_{s \in \mathcal{D}_r} |\mu(s)\mu(ks/r)| \frac{r}{k^3 s^3} \Big). \end{aligned} \tag{5.1}$$

Here we have applied the inequalities $T_r \ll 1/r$ (Lemma 3.2) and

$$J_3(n) = n^3 \prod_{p|n} \Big(1 - \frac{1}{p^3}\Big) > n^3 \prod_{p \in \mathbb{P}} \Big(1 - \frac{1}{p^3}\Big) = \frac{n^3}{\zeta(3)} \qquad (n \geq 1) \tag{5.2}$$

(see [8, Theorem 280]). In order to estimate $k^3 s^3/r$ we discuss the following two cases. Recall that $r|k$ and $s|r$, and that the number P is the smallest prime divisor of k.

Case 1: $1 \leq r < k$ and $s = 1$.

$$\frac{k^3 s^3}{r} = \frac{k^3}{r} \geq \frac{k^3}{k/P} = Pk^2\,.$$

Case 2: $1 \leq r \leq k$ and $s \geq P$.

$$\frac{k^3 s^3}{r} \geq \frac{k^3 s^3}{k} \geq P^3 k^2 \geq Pk^2\,.$$

Using these bounds we estimate the error term in (5.1). This gives

$$\begin{aligned}\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha &= \frac{T_k}{\zeta(3)k} + \mathcal{O}\Big(\sum_{\substack{r \in \mathcal{D}_k \\ r \neq k \vee s \neq 1}} \sum_{s \in \mathcal{D}_r} |\mu(s)\mu(ks/r)| \frac{1}{Pk^2} \Big) \\ &= \frac{T_k}{\zeta(3)k} + \mathcal{O}\Big(\frac{1}{Pk^2} \sum_{r \in \mathcal{D}_k} \sum_{s \in \mathcal{D}_r} |\mu(s)\mu(ks/r)| \Big) \\ &= \frac{\zeta(2)}{2\zeta(3)k^2} + \mathcal{O}\Big(\frac{1}{k^3}\Big) + \mathcal{O}\Big(\frac{1}{Pk^2} \sum_{r \in \mathcal{D}_k} \sum_{s \in \mathcal{D}_r} |\mu(s)\mu(ks/r)| \Big), \end{aligned}$$

where we have applied the asymptotic formula for T_k from Lemma 3.2. To complete the proof of the corollary we finally prove the identity

$$q_k := \sum_{r\in\mathcal{D}_k}\sum_{s\in\mathcal{D}_r} |\mu(s)\mu(ks/r)| \;=\; 3^t \qquad (k = p_1^{a_1}\cdots p_t^{a_t})$$

by induction with respect to t. For $t = 1$ let $k = p^a$. We count three pairs $[r,s] \in \mathcal{D}_k \times \mathcal{D}_r$ such that $|\mu(s)\mu(ks/r)| = 1$ given by $[p^a,1]$, $[p^a,p]$, and $[p^{a-1},1]$. Now we assume that $q_{k'} = 3^t$ holds for all integers k' having t prime divisors. Let $k = p_1^{a_1}\cdots p_t^{a_t}p_{t+1}^{a_{t+1}}$ and $k' = p_1^{a_1}\cdots p_t^{a_t}$. While $[r',s'] \in \mathcal{D}_{k'} \times \mathcal{D}_{r'}$ runs through all 3^t pairs which are counted for $q_{k'}$, we obtain q_k by counting the $3\cdot 3^t$ pairs $[r,s] \in \mathcal{D}_k \times \mathcal{D}_r$ given by $[r'p_{t+1}^{a_t+1}, s']$, $[r'p_{t+1}^{a_{t+1}}, s'p_{t+1}]$, and $[r'p_{t+1}^{a_{t+1}-1}, s']$. This completes the proof of Corollary 2.2. □

Proof of Corollary 2.3 For $k = p \in \mathbb{P}$ the multiple sum in Theorem 2.1 consists of three terms corresponding to $[r = 1, s = 1]$, $[r = p, s = 1]$, and $[r = p, s = p]$. Therefore, we obtain

$$\int_0^1 \mathcal{E}_p(\alpha)\,d\alpha \;=\; \frac{1}{\zeta(3)}\Big(-\frac{T_1}{J_3(p)} + \frac{T_p}{p} + \frac{T_p}{pJ_3(p)}\Big).$$

With $J_3(p) = p^3 - 1$ and

$$T_1 \;=\; \frac{3}{2}\zeta(2)\log 2 - \frac{1}{4}\zeta(3)$$

given in Lemma 3.2 we prove the identity stated in the corollary. Now, for $p \ge 3$ we have with Lemma 3.2:

$$\int_0^1 \mathcal{E}_p(\alpha)\,d\alpha \;<\; \frac{1}{p^3-1}\Big(\frac{p^2}{(p-1)\zeta(3)} - \frac{3\zeta(2)\log 2}{2\zeta(3)} + \frac{1}{4}\Big) \;<\; \frac{97}{109p^2},$$

and

$$\int_0^1 \mathcal{E}_p(\alpha)\,d\alpha \;>\; \frac{1}{p^3-1}\Big(\frac{p}{2\zeta(3)} - \frac{3\zeta(2)\log 2}{2\zeta(3)} + \frac{1}{4}\Big) \;>\; \frac{2}{77p^2}.$$

This proves the inequalities stated in Corollary 2.3. □

Proofs of Corollaries 2.4 and 2.5 We apply Corollary 2.2 with $k = p^a$, $t = 1$, and $P = p$. Then the error term in Corollary 2.2 takes the form

$$\mathcal{O}\Big(\frac{1}{k^3} + \frac{3^t}{k^2P}\Big) \;=\; \mathcal{O}\Big(\frac{1}{k^3} + \frac{1}{k^2p}\Big) \;=\; \mathcal{O}\Big(\frac{1}{k^3} + \frac{1}{k^2k^{1/a}}\Big) \;=\; \mathcal{O}\Big(\frac{1}{k^{2+1/a}}\Big).$$

Thus Corollary 2.4 is proven. Also Corollary 2.5 follows immediately from Corollary 2.2. □

6 Proofs of Theorems 2.6 and 2.7

Proof of Theorem 2.6 For the upper bound we estimate the right-hand side of the identity in (4.3). Let $k \geq 2$. Then

$$\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha = \sum_{m=1}^{\infty} \sum_{\substack{b=1 \\ (km,b)=1}}^{km-1} \frac{1}{km(km+b)^2} < \sum_{m=1}^{\infty} \sum_{b=1}^{km-1} \frac{1}{k^3m^3} < \sum_{m=1}^{\infty} \frac{1}{k^2m^2} = \frac{\zeta(2)}{k^2}.$$

On the other hand, the lower bound for the integral in Theorem 2.6 follows from the identity (4.3), too. Here we assume that $k \geq 3$.

$$\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha \geq \sum_{\substack{b=1 \\ (k,b)=1}}^{k-1} \frac{1}{k(k+b)^2} \geq \frac{\varphi(k)}{k(2k-1)^2} > \frac{\varphi(k)}{4k^3} \gg \frac{1}{k^2 \log\log k}. \tag{6.1}$$

The inequality on the right-hand side involving a lower bound of Euler's totient follows from Theorem 328 in [8].

Next, let $k = p_1p_2\cdots p_r$ for some positive integer $r \geq 2$. Then we have

$$\log k = \sum_{\substack{p \leq p_r \\ p \in \mathbb{P}}} \log p = \vartheta(p_r) \ll p_r$$

by Theorem 414 in [8]. Applying additionally Theorem 429 in [8], we obtain

$$\prod_{\substack{p|k \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right) = \prod_{\substack{p \leq p_r \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right) \ll \frac{1}{\log p_r} \ll \frac{1}{\log\log k}. \tag{6.2}$$

Moreover,

$$\begin{aligned}
\int_0^1 \mathcal{E}_k(\alpha)\,d\alpha &\leq \sum_{m=1}^{\infty} \sum_{\substack{b=1 \\ (km,b)=1}}^{km-1} \frac{1}{k^3m^3} = \frac{1}{k^3} \sum_{m=1}^{\infty} \frac{\varphi(km)}{m^3} \\
&= \frac{1}{k^2} \sum_{m=1}^{\infty} \frac{1}{m^2} \prod_{\substack{p|km \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right) \leq \frac{\zeta(2)}{k^2} \prod_{\substack{p|k \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p}\right) \\
&\ll \frac{1}{k^2 \log\log k} \qquad \text{(by (6.2))}.
\end{aligned}$$

Together with the lower bound (6.1) we complete the proof of the theorem. □

Proof of Theorem 2.7 By (4.2) we have already shown the identities in the theorem. So it remains to prove the inequalities. First, we prove the upper bounds.

$$\begin{aligned}
&\sum_{\substack{a=1\\ a\equiv l \pmod k}}^{\infty}\ \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} - \frac{3\chi_{k,l}(1)}{8}\\
&= \sum_{m=0}^{\infty}\ \sum_{\substack{b=0\\ (km+l,b)=1}}^{km+l-1} \frac{1}{(km+l)(km+l+b)^2} - \frac{3\chi_{k,l}(1)}{8}\\
&\le \sum_{m=0}^{\infty}\sum_{b=0}^{km+l-1} \frac{1}{(km+l)^3} - \frac{3\chi_{k,l}(1)}{8} = \frac{1}{l^2} + \sum_{m=1}^{\infty}\frac{1}{(km+l)^2} - \frac{3\chi_{k,l}(1)}{8}\\
&\le \frac{1}{l^2} + \sum_{m=1}^{\infty}\frac{1}{k^2m^2} - \frac{3\chi_{k,l}(1)}{8} = \frac{1}{l^2} + \frac{\zeta(2)}{k^2} - \frac{3\chi_{k,l}(1)}{8}\\
&= \begin{cases} \dfrac{5}{8} + \dfrac{\zeta(2)}{k^2} & \text{if } l=1\,,\\[2ex] \dfrac{1}{l^2} + \dfrac{\zeta(2)}{k^2} & \text{if } l>1\,. \end{cases}
\end{aligned}$$

For the lower bounds we treat the cases $l = 1$ and $l > 1$ separately. First, let $l = 1$. Then

$$\begin{aligned}
&\sum_{\substack{a=1\\ a\equiv 1 \pmod k}}^{\infty}\ \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} - \frac{3\chi_{k,1}(1)}{8}\\
&= \sum_{m=0}^{\infty}\ \sum_{\substack{b=0\\ (km+1,b)=1}}^{km} \frac{1}{(km+1)(km+1+b)^2} - \frac{3}{8}\\
&= \frac{5}{8} + \sum_{m=1}^{\infty}\ \sum_{\substack{b=0\\ (km+1,b)=1}}^{km} \frac{1}{(km+1)(km+1+b)^2}\\
&\ge \frac{5}{8} + \sum_{\substack{b=1\\ (k+1,b)=1}}^{k} \frac{1}{(k+1)(k+1+b)^2}\\
&> \frac{5}{8} + \sum_{\substack{b=1\\ (k+1,b)=1}}^{k+1} \frac{1}{4(k+1)^3} = \frac{5}{8} + \frac{\varphi(k+1)}{4(k+1)^3}\,.
\end{aligned}$$

Next, let $l > 1$. Then

$$\sum_{\substack{a=1\\ a\equiv l \pmod k}}^{\infty} \sum_{\substack{b=0\\ (a,b)=1}}^{a-1} \frac{1}{a(a+b)^2} - \frac{3\chi_{k,1}(1)}{8}$$

$$= \sum_{m=0}^{\infty} \sum_{\substack{b=1\\ (km+l,b)=1}}^{km+l-1} \frac{1}{(km+l)(km+l+b)^2}$$

$$\geq \sum_{\substack{b=1\\ (l,b)=1}}^{l-1} \frac{1}{l(l+b)^2} > \sum_{\substack{b=1\\ (l,b)=1}}^{l} \frac{1}{4l^3} = \frac{\varphi(l)}{4l^3}.$$

This completes the proof of the theorem. □

References

1. D.H. Bailey, J.M. Borwein, N.J. Calkin, R. Girgensohn, D.R. Luke, V.H. Moll, *Experimental Mathematics in Action* (A.K. Peters, CRC Press, Wellesley, Massachusetts, 2007)
2. J.M. Borwein, I.J. Zucker, J. Boersma, The evaluation of character Euler double sums. Ramanujan J. **15**, 377–405 (2008)
3. C. Elsner, On the approximation of irrationals by rationals. Math. Nachr. **189**, 243–256 (1998)
4. C. Elsner, On arithmetic properties of the convergents of Euler's number. Colloq. Math. **79**, 133–145 (1999)
5. C. Elsner, Series of error terms for rational approximations of irrational numbers. J. Integer Seq. **14** (2011). Article 11.1.4. http://www.cs.uwaterloo.ca/journals/JIS/VOL14/Elsner/elsner9.html
6. C. Elsner, M. Stein, On error sum functions formed by convergents of real numbers. J. Integer Seq. **14** (2011). Article 11.8.6; http://www.cs.uwaterloo.ca/journals/JIS/VOL14/Elsner2/elsner10.html
7. C. Elsner, M. Stein, On the value distribution of Error Sums for approximations with rational numbers. Integers **12**, 1–28 (2012). A66.
8. G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edn. (Clarendon Press, Oxford, 1979)
9. T. Komatsu, Arithmetical properties of the leaping convergents of $e^{1/s}$. Tokyo J. Math. **27**(1), 1–12 (2004)
10. D. Suryanarayana, The greatest divisor of n which is prime to k. Math. Student **37**, 147–152 (1969)
11. S. Uchiyama, On rational approximations to irrational numbers. Tsukuba J. Math. **4**, 1–7 (1980)

Sum of the Lerch Zeta-Function over Nontrivial Zeros of the Dirichlet *L*-Function

Ramūnas Garunkštis and Justas Kalpokas

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract For $0 < \alpha \leq 1$ and $0 < \lambda \leq 1$, λ rational, we consider the sum of values of the Lerch zeta-function $L(\lambda, \alpha, s)$ taken at the nontrivial zeros of the Dirichlet L-function $L(s, \chi)$, where χ mod Q, $Q \geq 1$, is a primitive Dirichlet character.

Keywords Dirichlet L-function • Value-distribution

2010 Mathematics subject classification: Primary 11M06; Secondary 11M26

1 Introduction

Let $s = \sigma + it$ denote a complex variable. We use the notation $e(x) = \exp(2\pi ix)$. By $\{x\}$, (a, b), and $[a, b]$ we denote the fractional part of the real number x, the greatest common divisor of integers a, b, and the least common multiple of integers a, b, respectively. In this paper T always tends to plus infinity and ε is any positive number.

The Lerch zeta-function is defined by

$$L(\lambda, \alpha, s) = \sum_{n=0}^{\infty} \frac{e(\lambda n)}{(n+\alpha)^s} \quad (\sigma > 1),$$

R. Garunkštis (✉) • J. Kalpokas
Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, 03225 Vilnius, Lithuania
e-mail: ramunas.garunkstis@mif.vu.lt; justas.kalpokas@mif.vu.lt

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_10

where $0 < \lambda \le 1$ and $0 < \alpha \le 1$. The Dirichlet L-function is defined by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (\sigma > 1),$$

where $\chi(n)$ is a Dirichlet character modulo some positive integer Q. For $\chi \bmod 1$ we get the Riemann zeta-function $L(s,\chi) = \zeta(s)$. The yet unsolved generalized Riemann hypothesis (GRH) states that inside the critical strip $0 < \sigma < 1$ every Dirichlet L-function has zeros only on the critical line $\sigma = \frac{1}{2}$. Zeros in the critical strip are called nontrivial and we denote them by $\rho_\chi = \beta_\chi + i\gamma_\chi$. In view of the functional equation (see formula (2.4) below) the nontrivial zeros are symmetrically distributed with respect to the critical line. A Dirichlet character $\chi \bmod Q$ is said to be primitive if it is not induced by any other character of modulus strictly less than Q. The unique principal character modulo Q is denoted by χ_0. The character $\chi_0 \bmod 1$ is the only one principal and primitive character. For $T > 0$, let $N(T,\chi)$ denote the number of the nontrivial zeros with $0 \le \gamma_\chi \le T$. For the primitive character $\chi \bmod Q$, we have (Montgomery and Vaughan [17, Corollary 14.7])

$$N(T,\chi) = \frac{T}{2\pi} \log \frac{QT}{2\pi e} + O(\log QT),$$

where $T \ge 4$.

For special values of α and λ the Lerch zeta-function reduces to the Riemann zeta-function $L(1,1,s) = \zeta(s)$, $L(1,1/2,s) = (2^s - 1)\zeta(s)$, $L(1/2,1,s) = (1-2^{1-s})\zeta(s)$, the Dirichlet L-function $L(1/2,1/2,s) = 2^s L(s,\psi)$, where $\psi \bmod 4$ is an odd Dirichlet character. If we fix $\lambda = 1$ we get the Hurwitz zeta-function $L(1,\alpha,s) = \zeta(s,\alpha)$ and if we fix $\alpha = 1$ we get the periodic zeta-function $e(\lambda)L(\lambda,1,s) = F(s,\lambda)$. Nontrivial zeros $\rho(\lambda,\alpha) = \beta(\lambda,\alpha) + i\gamma(\lambda,\alpha)$ of the Lerch zeta-function $L(\lambda,\alpha,s)$ are located in the strip $-1 < \sigma < 1+\alpha$ ([9]). In view of the formula [8, Corollary 2]

$$\sum_{|\gamma(\lambda,\alpha)| \le T} \left(\beta(\lambda,\alpha) - \frac{1}{2} \right) = \frac{T}{2\pi} \log \frac{\alpha}{\sqrt{\lambda(1-\{\lambda\})}} + O(\log T),$$

we see that the nontrivial zeros are not always symmetrically distributed with respect to the critical line. It is pleasant to recall that the paper [8] was written when the first author was visiting W. Schwarz at Frankfurt university.

Let

$$\Lambda(x) = \begin{cases} \log p & \text{if } x = p^k \text{ for some prime } p \text{ and integer } k \ge 1, \\ 0 & \text{otherwise} \end{cases}$$

be the von Mangoldt function. For an integer n and a character χ mod Q the Gauss sum is defined by

$$G(n,\chi)=\sum_{a=1}^{Q}\chi(a)\exp\left(2\pi i\frac{an}{Q}\right).$$

If $(n,Q)=1$, then for a primitive character χ mod Q, we have $|G(n,\chi)|=\sqrt{Q}$ and, for the principle character χ_0 mod Q, it is known that $G(n,\chi_0)=\mu(n)$, where $\mu(n)$ is the Möbius function. We shall prove the following result:

Theorem 1.1 *Let χ mod Q, $Q\geq 1$, be a primitive Dirichlet character.*
We have, for $0<\lambda=\frac{k}{q}\leq 1$, $(k,q)=1$, and $0<\alpha<1$,

$$\sum_{0<\gamma_\chi\leq T}L\left(\lambda,\alpha,\rho_\chi\right)=-\left(\Lambda\left(\frac{1}{\alpha}\right)\chi\left(\frac{1}{\alpha}\right)+\delta(Q,q)e\left(-\alpha\lambda\right)\frac{\mu(q)}{\phi(q)}L(1-\alpha,\lambda,1)\right)\frac{T}{2\pi}$$
$$+O\left(T\exp(-c\log^{\frac{1}{4}-\epsilon}T)\right),\tag{1.1}$$

where $\delta(Q,q)=1$ if $Q|q$, $\delta(Q,q)=0$ otherwise, and c is a positive absolute constant.

Further, for $0<\lambda=\frac{k}{q}<1$, $(k,q)=1$,

$$\sum_{0<\gamma_\chi\leq T}L(\lambda,1,\rho_\chi)=\frac{T}{2\pi}\log\frac{TQ}{2\pi e}-\delta(Q,q)e(-\lambda)\frac{\mu(q)}{\phi(q)}\frac{T}{2\pi}\log\frac{T}{2\pi e}+C(\chi,\lambda)\frac{T}{2\pi}$$
$$+O\left(T\exp(-c\log^{\frac{1}{4}-\epsilon}T)\right),\tag{1.2}$$

where the constant $C(\chi,\lambda)$ is defined by Eq. (2.17) below.

Let A be a positive constant. Both asymptotic formulas of this theorem are valid uniformly for $Q\ll\log^A T$.

Next we discuss the asymptotic formula (1.1) of Theorem 1.1. From the proof of Theorem 1.2 in Nakamura [18] we know that, for $0<\lambda<1$ and $0<\alpha\leq 1$,

$$L(\lambda,\alpha,1)\neq 0.$$

The proof of the last formula is nice and short. By the integral representation (Lerch [16, formula (2)] or [15, formula (2.6)]) we have

$$\Gamma(\sigma)L(\lambda,\alpha,\sigma)=\int_0^\infty\frac{x^{\sigma-1}e^{(1-\alpha)x}}{e^x-e^{2\pi i\lambda}}dx=\int_0^\infty\frac{x^{\sigma-1}e^{(1-\alpha)x}(e^x-e^{-2\pi i\lambda})}{|e^x-e^{2\pi i\lambda}|^2}dx\quad(\sigma>0).$$

Now $\mathrm{Re}\,L(\lambda,\alpha,1)>0$ since $\mathrm{Re}\,(e^{(1-\alpha)x}(e^x-e^{2\pi i\lambda}))>0$ for $x>0$.

Formula (1.1) extends results obtained in Fujii [4], Steuding [10, 21], where the case $\lambda=1$, $0<\alpha<1$, and $Q=1$ was investigated. In [6] and [14] Formula (1.2)

with $0 < \lambda = k/q < 1$, $(k, q) = 1$, $\alpha = 1$, and $Q = 1$ was considered, see also Steuding [22].

In the paper [11] the sum of $L(s, \chi)$ and in [7] the sum of $L(s, \chi)L(1 - s, \chi)$ over nontrivial zeros of another Dirichlet L-function were studied.

The next section is devoted to the proof of Theorem 1.1.

2 Proof of Theorem 1.1

We will use contour integration. The proof of the theorem relies on the method of Conrey et al. [2]. We divide the proof into the following Sects.: 2.1. Beginning of the proof: Functional equations; Sect. 2.2. Gonek's lemma; and Sect. 2.3. Perron's formula.

2.1 Beginning of the Proof: Functional Equations

Similarly as in [11], without loss of generality, we consider T satisfying the inequality

$$\min_{\gamma_\chi} |T - \gamma_\chi| \gg \frac{1}{\log(QT)}. \tag{2.1}$$

For $q \geq 1$, $\chi \bmod q$ and $t \geq 0$ we have (Prachar [20, Theorem 3.3 in Chap. 7])

$$N_\chi(t + 1) - N_\chi(t) := \#\{\rho_\chi = \beta_\chi + i\gamma_\chi \,:\, t < \gamma_\chi \leq t + 1\} \ll \log Q(t + 2).$$

Thus

$$\sum_{0<\gamma_\chi\leq T} L(\lambda, \alpha, \rho_\chi) = \frac{1}{2\pi i} \int_{\mathfrak{C}} \frac{L'}{L}(s, \chi)L(\lambda, \alpha, s)ds + O(\log Q),$$

where the contour $\mathfrak{C}$ is a rectangle with vertices $a + ib$, $a + iT$, $1 - a + iT$, and $1 - a + ib$, where $a = 1 + 1/\log(QT)$, $2 \leq b \leq 3$, $\min_{\gamma_\chi} |b - \gamma_\chi| \gg 1/\log Q$. Further

$$\begin{aligned}
&\frac{1}{2\pi i} \int_{\mathfrak{C}} \frac{L'}{L}(s, \chi)L(\lambda, \alpha, s)ds \\
&= \frac{1}{2\pi i} \left\{ \int_{a+ib}^{a+iT} + \int_{a+iT}^{1-a+iT} + \int_{1-a+iT}^{1-a+ib} + \int_{1-a+ib}^{a+ib} \right\} \frac{L'}{L}(s, \chi)L(\lambda, \alpha, s)ds \\
&=: \sum_{j=1}^{4} \mathcal{J}_j.
\end{aligned}$$

First we obtain

$$\begin{aligned}\mathcal{J}_1 =& \frac{1}{2\pi i}\int_{a+ib}^{a+iT}\frac{L'}{L}(s,\chi)L(\lambda,\alpha,s)ds\\ =& \frac{1}{2\pi}\int_b^T \frac{L'}{L}(a+it,\chi)L(\lambda,\alpha,a+it)dt\\ =& -\sum_{m=2}^{\infty}\sum_{n=0}^{\infty}\frac{\chi(m)\Lambda(m)e(\lambda n)}{(m(n+\alpha))^a}\frac{1}{2\pi}\int_b^T\frac{1}{(m(n+\alpha))^{it}}dt\\ =& -\Lambda\left(\frac{1}{\alpha}\right)\chi\left(\frac{1}{\alpha}\right)\frac{T}{2\pi}+O(\log^2(QT)).\end{aligned}$$

Second we consider $\mathcal{J}_2$. Formula (6) from [11] gives [recall that T satisfies (2.1)]

$$\frac{L'}{L}(\sigma+iT,\chi)\ll\log^2(QT)\qquad\text{for}\quad -1\le\sigma\le 2, T\ge 2. \tag{2.2}$$

By Corollary 4 from [5] we have

$$L(\lambda,\alpha,\sigma+iT)\ll T^{\frac{1}{2}}\log T\qquad\text{for}\quad -\frac{1}{\log(QT)}\le\sigma\le 1+\frac{1}{\log(QT)}. \tag{2.3}$$

Thus we get

$$\mathcal{J}_2=\frac{1}{2\pi i}\int_{a+iT}^{1-a+iT}\frac{L'}{L}(s,\chi)L(\lambda,\alpha,s)ds=O\left(T^{\frac{1}{2}}\log^3(QT)\right).$$

Similarly we see that

$$\mathcal{J}_4=O(\log^3 Q).$$

A change of variables $s\mapsto 1-\overline{s}$ gives

$$\mathcal{J}_3=-\frac{1}{2\pi i}\int_{a+ib}^{a+iT}\frac{L'}{L}(1-\overline{s},\chi)L(\lambda,\alpha,1-\overline{s})ds.$$

After conjugation we get

$$\overline{\mathcal{J}_3}=-\frac{1}{2\pi i}\int_{a+ib}^{a+iT}\frac{L'}{L}(1-s,\overline{\chi})\overline{L(\lambda,\alpha,1-\overline{s})}ds.$$

To evaluate this integral we will use functional equations. A Dirichlet L-function to a primitive character χ mod Q satisfies the functional equation (Apostol [1, Theorem 12.11])

$$L(1-s,\chi) = \Delta(1-s,\chi)L(s,\overline{\chi}), \tag{2.4}$$

where

$$\Delta(1-s,\chi) = \tau(\psi)\frac{1}{Q}\left(\frac{Q}{2\pi}\right)^s \Gamma(s)\left(\exp\left(-\frac{\pi i s}{2}\right) + \psi(-1)\exp\left(\frac{\pi i s}{2}\right)\right).$$

Taking the logarithmic derivative of the functional equation we get

$$\frac{L'}{L}(1-s,\chi) = \frac{\Delta'}{\Delta}(1-s,\chi) - \frac{L'}{L}(s,\overline{\chi}),$$

where

$$\frac{\Delta'}{\Delta}(s,\chi) = \frac{\Delta'}{\Delta}(1-s,\overline{\chi}) = -\log\frac{tQ}{2\pi} + O\left(\frac{1}{t}\right), \tag{2.5}$$

for $t > 1$. The Lerch zeta-function satisfies the functional equation (Lerch [16] or [15])

$$\begin{aligned} L(\lambda,\alpha,1-s) =& (2\pi)^{-s}\Gamma(s)\Big(e\left(\frac{s}{4}-\alpha\lambda\right)L(1-\alpha,\lambda,s) \\ &+ e\left(-\frac{s}{4}+\alpha(1-\{\lambda\})\right)L(\alpha,1-\{\lambda\},s)\Big). \end{aligned} \tag{2.6}$$

Therefore

$$\begin{aligned} &\frac{L'}{L}(1-s,\overline{\chi})\overline{L(\lambda,\alpha,1-\overline{s})} \\ &= \left(\frac{\Delta'}{\Delta}(s,\chi) - \frac{L'}{L}(s,\chi)\right)(2\pi)^{-s}\Gamma(s)\Big(e\left(-\frac{s}{4}+\alpha\lambda\right)L(\alpha,\lambda,s) \\ &\quad + e\left(\frac{s}{4}-\alpha(1-\{\lambda\})\right)L(1-\alpha,1-\{\lambda\},s)\Big). \end{aligned}$$

Then

$$\begin{aligned} \overline{\mathcal{J}_3} =& -e(\alpha\lambda)\frac{1}{2\pi i}\int_{a+ib}^{a+iT}\frac{\Delta'}{\Delta}(s,\chi)(2\pi)^{-s}\Gamma(s)e\left(-\frac{s}{4}\right)L(\alpha,\lambda,s)ds \\ &- e(-\alpha(1-\{\lambda\}))\frac{1}{2\pi i}\int_{a+ib}^{a+iT}\frac{\Delta'}{\Delta}(s,\chi)(2\pi)^{-s}\Gamma(s)e\left(\frac{s}{4}\right)L(1-\alpha,1-\{\lambda\},s)ds \end{aligned}$$

$$+ e(\alpha\lambda)\frac{1}{2\pi i}\int_{a+ib}^{a+iT}(2\pi)^{-s}\Gamma(s)e\left(-\frac{s}{4}\right)\frac{L'}{L}(s,\chi)L(\alpha,\lambda,s)ds$$

$$+ e(-\alpha(1-\{\lambda\}))\frac{1}{2\pi i}\int_{a+ib}^{a+iT}(2\pi)^{-s}\Gamma(s)e\left(\frac{s}{4}\right)\frac{L'}{L}(s,\chi)L(1-\alpha,1-\{\lambda\},s)ds$$

$$=:\sum_{j=1}^{4}\mathcal{F}_j,$$

say. In view of the bound (2.5), Stirling's formula, and by the bound [5, Corollary 2]

$$L(\lambda,\alpha,a+it)\ll\log t, \tag{2.7}$$

we have

$$\mathcal{F}_2,\mathcal{F}_4\ll 1.$$

Summarizing the so far obtained results we see that, for $0<\lambda\le 1$, $0<\alpha\le 1$, and $Q\ge 1$,

$$\sum_{0<\gamma_\chi\le T}L(\lambda,\alpha,\rho_\chi)=-\Lambda\left(\frac{1}{\alpha}\right)\chi\left(\frac{1}{\alpha}\right)\frac{T}{2\pi}+\overline{\mathcal{F}_1}+\overline{\mathcal{F}_3}+O(T^{1/2+\epsilon}). \tag{2.8}$$

2.2 Gonek's Lemma

For $\mathcal{F}_1$ and $\mathcal{F}_3$ we will use the following version of Gonek's Lemma (c.f. Gonek [12, Lemma 5] and [3, Lemma 2]).

Lemma 2.1 *Assume that* $\sum_{m\le x}|a_m|\ll x$ *and* $b_n\ll 1$. *Let* $1<c\le 1+1/\log\tau$ *and* $0<\delta<1$, *then*

$$\frac{1}{2\pi i}\int_{c+i}^{c+i\tau}\Delta(1-s)\sum_{m=1}^{\infty}\frac{a_m}{m^s}\sum_{n=0}^{\infty}\frac{b_n}{(n+\alpha)^s}ds$$

$$=\sum_{\substack{m\ge 1,n\ge 0\\ m(n+\alpha)\le\frac{\tau}{2\pi}}}a_mb_ne(-m(n+\alpha))+O\left(\tau^{\frac{1}{2}}(c-1)^{-2}\right)$$

uniformly in $\alpha\in[\delta,1]$. *Here*

$$\Delta(1-s)=2(2\pi)^{-s}\Gamma(s)\cos\frac{\pi s}{2}$$

is a factor from the functional equation $\zeta(1-s)=\Delta(1-s)\zeta(s)$.

Proof This is Lemma 5 in [10].

Let $\delta = \pm 1$. In order to apply Lemma 2.1 for our purpose note that

$$\frac{e\left(\delta\frac{s}{4}\right)}{2\cos\frac{\pi s}{2}} = \begin{cases} O\left(\exp\left(-\pi|t|\right)\right) & \text{if } \delta t \geq 0, \\ 1 + O\left(\exp\left(-\pi|t|\right)\right) & \text{otherwise.} \end{cases} \tag{2.9}$$

We return to the integral $\mathcal{F}_1$ and rewrite it as follows:

$$\mathcal{F}_1 = -e(\alpha\lambda)\int_b^T \frac{\Delta'}{\Delta}(a+i\tau,\chi)\,d\left(\frac{1}{2\pi i}\int_{a+i}^{a+i\tau}(2\pi)^{-s}\Gamma(s)e\left(-\frac{s}{4}\right)L(\alpha,\lambda,s)ds\right).$$

In view of (2.9) and the bound from (2.7) Lemma 2.1 gives

$$\begin{aligned}&\frac{1}{2\pi i}\int_{a+i}^{a+i\tau}(2\pi)^{-s}\Gamma(s)e\left(-\frac{s}{4}\right)L(\alpha,\lambda,s)ds \\ &= \sum_{0\leq n\leq\frac{\tau}{2\pi}-\lambda} e(\alpha n)e(-(n+\lambda)) + O(\tau^{\frac{1}{2}+\epsilon}) \\ &= e(-\lambda)\sum_{0\leq n\leq\frac{\tau}{2\pi}-\lambda} e(\alpha n) + O(\tau^{\frac{1}{2}+\epsilon}) = O(\tau^{\frac{1}{2}+\epsilon}).\end{aligned}$$

Then using Expression (2.5) we have, for $\alpha \neq 1$,

$$\mathcal{F}_1 = -e(\alpha\lambda)\int_b^T \frac{\Delta'}{\Delta}(a+i\tau,\chi)\,d\left(O(\tau^{\frac{1}{2}+\epsilon})\right) = O(T^{1/2+\epsilon})$$

and, for $\alpha = 1$,

$$\mathcal{F}_1 = \frac{T}{2\pi}\log\frac{TQ}{2\pi e} + O(T^{1/2+\epsilon}).$$

Next we consider the integral $\mathcal{F}_3$. Again by formula (2.9) and Lemma 2.1 we get

$$\mathcal{F}_3 = -e(\alpha\lambda)\sum_{\substack{m\geq 1,n\geq 0\\ m(n+\lambda)\leq\frac{T}{2\pi}}} \Lambda(m)\chi(m)e(\alpha n)e(-m(n+\lambda)) + O(T^{1/2+\epsilon}).$$

We split the last sum into two sums with $(m,q) = 1$ and $(m,q) > 1$ accordingly. For the case $(m,q) > 1$ we obtain, for $\alpha \neq 1$,

$$\sum_{\substack{m\geq 1,n\geq 0,(m,q)>1\\ m(n+\lambda)\leq\frac{T}{2\pi}}} \Lambda(m)\chi(m)e(\alpha n)e(-m\lambda) = O\left(\sum_{\substack{m\leq\frac{T}{2\pi}\\ (m,q)>1}}\Lambda(m)\right) = O(\log T)$$

and, for $\alpha = 1$,

$$\sum_{\substack{m\geq 1,n\geq 0,(m,q)>1\\ m(n+\lambda)\leq \frac{T}{2\pi}}} \Lambda(m)\chi(m)e(\alpha n)e(-m\lambda) = \frac{T}{2\pi}\sum_{\substack{m\leq \frac{T}{2\pi}\\ (m,q)>1}} \Lambda(m)\chi(m)e(-m\lambda)\frac{1}{m} + O(\log T)$$

$$= \frac{T}{2\pi}\sum_{p|q}\log p\sum_{j=1}^{\infty}\frac{\chi(p^j)e(-p^j\lambda)}{p^j} + O(\log T).$$

Now we use that $\lambda = \frac{k}{q}$. If $(m,q) = 1$, then the orthogonality relation for Dirichlet characters gives

$$\Lambda(m)\chi(m)e\left(-m\frac{k}{q}\right) = \frac{1}{\phi(q)}\sum_{\psi \bmod q}\sum_{a=1}^{q}\overline{\psi}(a)e\left(-a\frac{k}{q}\right)\Lambda(m)\chi(m)\psi(m)$$

$$= \frac{1}{\phi(q)}\sum_{\psi \bmod q} G(-k,\overline{\psi})\Lambda(m)\chi(m)\psi(m),$$

where $G(-k,\overline{\psi})$ is the Gauss sum defined before Theorem 1.1. Then, for $0 < \alpha \leq 1$,

$$\mathcal{F}_3 = -\frac{e(\alpha\lambda)}{\phi(q)}\sum_{\psi \bmod q} G(-k,\overline{\psi})\sum_{\substack{m\geq 1,n\geq 0\\ m(n+\lambda)\leq \frac{T}{2\pi}}}\Lambda(m)\chi(m)\psi(m)e(\alpha n) \tag{2.10}$$

$$-(\alpha - \{\alpha\})e(\lambda)\frac{T}{2\pi}\sum_{p|q}\log p\sum_{j=1}^{\infty}\frac{\chi(p^j)e(-p^j\lambda)}{p^j} + O(T^{1/2+\epsilon}).$$

Again, we summarize obtained results. In view of formula (2.8) Sect. 2.2 gives, for $0 < \lambda \leq 1$, $0 < \alpha \leq 1$, and $Q \geq 1$,

$$\sum_{0<\gamma_\chi\leq T} L(\lambda,\alpha,\rho_\chi) = (\alpha - \{\alpha\})\frac{T}{2\pi}\log\frac{TQ}{2\pi e} - \Lambda\left(\frac{1}{\alpha}\right)\chi\left(\frac{1}{\alpha}\right)\frac{T}{2\pi} + \overline{\mathcal{F}_3} + O(T^{1/2+\varepsilon}). \tag{2.11}$$

2.3 Perron's Formula

In Titchmarsh [23, Lemma 3.12] Perron's formula for ordinary Dirichlet series is proved. Easy to check that the analogous lemma is true for Dirichlet series $\frac{L'}{L}(s,\chi\psi)L(\alpha,\lambda,s)$. Note that Perron [19] proved his formula (without error term) for general Dirichlet series. Therefore, for the second sum of the formula (2.10),

Perron's formula gives

$$\sum_{\substack{m\geq 1,n\geq 0\\ m(n+\lambda)\leq \frac{T}{2\pi}}} \Lambda(m)\chi(m)\psi(m)e(\alpha n) = -\frac{1}{2\pi i}\int_{a-iU}^{a+iU}\frac{L'}{L}(s,\chi\psi)L(\alpha,\lambda,s)\left(\frac{T}{2\pi}\right)^s\frac{ds}{s} + O\left(\frac{T\log^2 T}{U}\right).$$

In [20, Chap. 8, Theorem 6.2] considering $[q,Q] \ll \log^B T$, with B being any positive constant, we find

$$L(s,\chi\psi)\neq 0 \quad \text{for} \quad \sigma > 1-\frac{c}{\log^{\frac{3}{4}+\epsilon} T},$$

where c is an absolute positive constant. With regard to this zero-free region for $L(s,\chi\psi)$ let $b_1 = 1 - c/\log^{(\frac{3}{4}+\epsilon)} T$. Shifting the line of integration we get

$$\begin{aligned}\sum_{\substack{m\geq 1,n\geq 0\\ m(n+\lambda)\leq \frac{T}{2\pi}}} \Lambda(m)\chi(m)\psi(m)e(\alpha n) &= -\mathrm{Res}_{s=1}\frac{L'}{L}(s,\chi\psi)L(\alpha,\lambda,s)\left(\frac{T}{2\pi}\right)^s\frac{1}{s}\\ &+\frac{1}{2\pi i}\left\{\int_{a+iU}^{b_1+iU}+\int_{b_1+iU}^{b_1-iU}+\int_{b_1-iU}^{a-iU}\right\}\frac{L'}{L}(s,\chi\psi)L(\alpha,\lambda,s)\left(\frac{T}{2\pi}\right)^s\frac{ds}{s} \qquad (2.12)\\ &+O\left(\frac{T\log^2 T}{U}\right)\\ &=: -\mathrm{Res}_{s=1}\frac{L'}{L}(s,\chi\psi)L(\alpha,\lambda,s)\left(\frac{T}{2\pi}\right)^s\frac{1}{s}+\mathcal{K}_1+\mathcal{K}_2+\mathcal{K}_3+O\left(\frac{T\log^2 T}{U}\right).\end{aligned}$$

Recall that the character χ is primitive. Thus if $\chi\psi$ is a principal character mod $[q,Q]$, then $Q|q$ and

$$\psi = \overline{\chi}\psi_0,$$

where ψ_0 is a principle character mod$q$. In view of this we introduce the notation

$$\delta(Q,q) = \begin{cases} 1 & \text{if } Q|q,\\ 0 & \text{otherwise.}\end{cases} \qquad (2.13)$$

The Dirichlet L-function attached to the principal character has a simple pole at $s=1$, otherwise it is an entire function. In view of $L(s,\psi_0) = \zeta(s)\prod_{p|q}(1-p^{-s})$

we have

$$\frac{L'}{L}(s,\psi_0) = -\frac{1}{s-1} + \gamma + \sum_{p|q} \frac{\log p}{p^s - 1} + O(s-1) \qquad (s \to 1),$$

here γ is the Euler–Mascheroni constant. For $0 < \alpha < 1$, the function $L(\alpha, \lambda, s)$ is entire and, for $\alpha = 1$, the function $L(\alpha, \lambda, s) = \zeta(s, \lambda)$ has a simple pole at $s = 1$. It is known (Ivić [13, formula (1.122)]) that

$$\zeta(s,\lambda) = \frac{1}{s-1} + \gamma(\lambda) + O(s-1) \qquad (s \to 1),$$

where

$$\gamma(\lambda) = \lim_{N\to\infty} \left(\sum_{m=0}^{N} \frac{1}{m+\lambda} - \log(N+\lambda) \right) = -\frac{\Gamma'(\lambda)}{\Gamma(\lambda)}.$$

The last equality can be found in Wilton [24]. Note that $\gamma(1)$ is the Euler–Mascheroni constant. Thus, for $\alpha \neq 1$,

$$-\operatorname{Res}_{s=1} \frac{L'}{L}(s,\psi_0) L(\alpha,\lambda,s) \left(\frac{T}{2\pi}\right)^s \frac{1}{s} = L(\alpha,\lambda,1)\frac{T}{2\pi} \tag{2.14}$$

and, for $\alpha = 1$,

$$-\operatorname{Res}_{s=1} \frac{L'}{L}(s,\psi_0) L(\alpha,\lambda,s) \left(\frac{T}{2\pi}\right)^s \frac{1}{s} = \frac{T}{2\pi}\log\frac{T}{2\pi e} - \left(\frac{\Gamma'(\lambda)}{\Gamma(\lambda)} + \gamma + \sum_{p|q} \frac{\log p}{p-1} \right) \frac{T}{2\pi}. \tag{2.15}$$

If $\chi\psi$ is a nonprincipal character mod$[q, Q]$, then for $\alpha = 1$,

$$-\operatorname{Res}_{s=1} \frac{L'}{L}(s,\chi\psi) L(\alpha,\lambda,s) \left(\frac{T}{2\pi}\right)^s \frac{1}{s} = -\frac{L'}{L}(1,\chi\psi)\frac{T}{2\pi}. \tag{2.16}$$

Integrals $\mathcal{K}_1$, $\mathcal{K}_2$, and $\mathcal{K}_3$ are analogous to the integrals which appear in Formula (9) of [11]. By a similar reasoning as in [11], using bounds (2.2), (2.3), and choosing $U = T^{1-b_1}$, we get that

$$\mathcal{K}_j \ll T^{1-\frac{c}{\log^{3/4+\varepsilon} T}},$$

for $j = 1, 2, 3$. In view of formulas (2.10)–(2.13) the residue (2.14) leads to Expression (1.1) of Theorem 1.1. Finally, residues (2.15) and (2.16) give (1.2) with

the constant

$$C(\chi,\lambda) = -\delta(Q,q)e(-\lambda)\frac{\mu(q)}{\phi(q)}\left(\frac{\Gamma'(\lambda)}{\Gamma(\lambda)} + \gamma + \sum_{p|q}\frac{\log p}{p-1}\right) + \\ + \frac{e(-\lambda)}{\phi(q)}\sum_{\substack{\psi \bmod q \\ \chi\psi \neq \psi_0}} G(k,\psi)\frac{L'}{L}(1,\overline{\chi\psi}) \\ -e(-\lambda)\sum_{p|q}\log p\sum_{j=1}^{\infty}\frac{\overline{\chi}(p^j)e(p^j\lambda)}{p^j}. \tag{2.17}$$

This proves Theorem 1.1.

Acknowledgement The authors are supported by grant No. MIP-049/2014 from the Research Council of Lithuania.

References

1. T.M. Apostol, *Introduction to Analytic Number Theory*, 5th edn. (Springer, New York, 1998)
2. J.B. Conrey, A. Ghosh, S.M. Gonek, Simple zeros of zeta functions. Publ. Math. Orsay **88**(02), 77–83 (1988)
3. J.B. Conrey, A. Ghosh, S.M. Gonek, Simple zeros of the Riemann zeta-function. Proc. Lond. Math. Soc. **76**(3), 497–522 (1998)
4. A. Fujii, Zeta zeros, Hurwitz zeta function and $L(1,\chi)$. Proc. Jpn. Acad. Ser. A **65**, 139–142 (1989)
5. R. Garunkštis, Approximation of the Lerch zeta-function. Lith. Math. J. **44**, 140–144 (2004)
6. R. Garunkštis, J. Kalpokas, Sum of the periodic zeta-function over the nontrivial zeros of the Riemann zeta-function. Analysis **28**, 209–217 (2008)
7. R. Garunkštis, J. Kalpokas, The discrete mean square of the Dirichlet L-function at nontrivial zeros of another Dirichlet L-function. Int. J. Number Theory **9**(4), 945–963 (2013)
8. R. Garunkštis, J. Steuding, On the zero distributions of Lerch zeta-functions. Analysis **22**, 1–12 (2002)
9. R. Garunkštis, J. Steuding, Do Lerch zeta-functions satisfy the Lindelof hypothesis?, in *Analytic and Probabilistic Methods in Number Theory (Palanga, 2001)* (TEV, Vilnius, 2002), pp. 61–74
10. R. Garunkštis, J. Steuding, On the distribution of zeros of the Hurwitz zeta-function. Math. Comp. **76**, 323–337 (2007)
11. R. Garunkštis, J. Kalpokas, J. Steuding, Sum of the Dirichlet L-function over nontrivial zeros of another Dirichlet L-function. Acta Math. Hungarica **128**(3), 287–298 (2010)
12. S.M. Gonek, Mean values of the Riemann zeta-function and its derivatives. Invent. Math. **75**, 123–141 (1984)
13. A. Ivić, *The Riemann Zeta-Function* (A Wiley-Interscience Publication, New York, 1985)
14. J. Kalpokas, Sum of the periodic zeta-function over the nontrivial zeros of the Riemann zeta-function, in *Proceedings of the Conference New Directions in the Theory of Universal Zeta and L Functions*, 6–10 October, 2008 (Shaker Verlag, Aachen, 2009), pp. 121–130
15. A. Laurinčikas, R. Garunkštis, *The Lerch Zeta-Function* (Kluwer Academic Publishers, Dordrecht, 2002)

16. M. Lerch, Note sur la fonction $\Re(w,x,s)=\sum_{k=0}^{\infty}\frac{e^{2k\pi ix}}{(w+k)^s}$. Acta Math. **11**, 287–298 (1887)
17. H.L. Montgomery, R.C. Vaughan, *Multiplicative Number Theory. I. Classical Theory.* Cambridge Studies in Advanced Mathematics, vol. 97 (Cambridge University Press, Cambridge, 2006)
18. T. Nakamura, Real zeros of Hurwitz-Lerch zeta and Hurwitz-Lerch type of Euler-Zagier double zeta functions. Math. Proc. Cambridge Philos. Soc. **160**(1), 39–50 (2016)
19. O. Perron, Zur Theorie der Dirichletschen Reihen. J. Reine Angew. Math. **134**, 95–143 (1908)
20. K. Prachar, *Primzahlverteilung* (Springer, Wien, 1957)
21. J. Steuding, On the value distribution of Hurwitz zeta-functions at the nontrivial zeros of the Riemann zeta-function. Abh. Math. Semin. Univ. Hamb. **71**, 113–121 (2001)
22. J. Steuding, Dirichlet series associated to periodic arithmetic functions and the zeros of Dirichlet *L* functions, in *Analytic and Probabilistic Methods in Number Theory* (TEV, Vilnius, 2002), pp. 282–296
23. E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, 2nd ed., revised by D.R. Heath-Brown (Oxford University Press, 1986)
24. J.R. Wilton, A note on the coefficients in the expansion of $\zeta(s,x)$ in powers of $s-1$. Quart. J. Pure Appl. Math. **50**, 329–332 (1927)

Schur–Weyl Dualities Old and New

Anne Henke

Dedicated to Wolfgang Schwarz, an inspiring teacher and mountaineering friend

Abstract We give an overview of Schur–Weyl dualities involved in the representation theory of orthogonal and symplectic groups and of the properties of a new class of algebras occurring in this context, the Brauer Schur algebras.

Keywords Brauer Schur algebras • Schur–Weyl duality

2010 Mathematics subject classification: Primary 16S50; Secondary 20G43

1 A Problem in Classical Invariant Theory

Let k be an algebraically closed field of any characteristic and G a general linear, orthogonal or symplectic group over k. A typical setup of classical invariant theory is to let the group G act on its *natural representation* E. Then it also acts on *tensor powers* of this natural representation E, on (tensor powers of) *exterior powers* and on (tensor powers of) *symmetric powers* of E.

Fundamental problem: What are the symmetries of such representations, that is, the endomorphism rings $\mathrm{End}_G(M)$, where M is one of these representations?

When addressing this problem, one tries to find *characteristic free* properties of the endomorphism rings, whose precise structure does in general depend on the characteristic of k. Moreover, one is hoping to find *double centraliser properties*: A bimodule ${}_AM_B$ over algebras A and B is said to satisfy the double centraliser property if

$$B \simeq \mathrm{End}_A(M) \text{ and } A \simeq \mathrm{End}_B(M).$$

A. Henke (✉)
Institut für Algebra und Zahlentheorie, Universität Stuttgart, Pfaffenwaldring 57, 70569 Stuttgart, Germany
e-mail: henke@mathematik.uni-stuttgart.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_11

Assuming that M is a left A-module for some algebra A, then M is also a right $B := \mathrm{End}_A(M)$-module via $m \cdot \varphi := \varphi(m)$ for any $m \in M$ and $\varphi \in B$, and the two actions on M commute. Without loss of generality we may assume that A acts faithfully on M, that is if $am = 0$ for all $m \in M$, then the element $a \in A$ must be zero. We then always have $A \subseteq \mathrm{End}_B(M)$ where $a \in A$ is mapped to the homomorphism multiplication with a, however, normally one cannot expect to have a set-equality, that is a double centraliser property. Generally, set-equality can only occur in case A (and B) acts *faithfully* on M. Therefore, when looking for double centraliser properties in our context, one has to define A as the largest quotient of the group algebra kG acting faithfully on the representation M. Since we choose M to be a finite dimensional vector space, the algebra A in a double centraliser property is a finite dimensional associative algebra. The given representation of G on M sends group elements to matrices acting k-linearly on M. The algebra A then is linearly generated by these matrices. The algebra A therefore is often called the *enveloping algebra* of the G-action on M. Sometimes, we will denote it by $S_{env}(G)$, when M is fixed.

When A happens to be a semisimple algebra, then M (finitely generated) by definition is a semisimple A-module. It affords a double centraliser property if and only if it is a faithful A-module. In this case, by Morita's theorem, there is an equivalence of categories between A-modules and B-modules, that is the algebras A and B have the same representation theory. The algebras we are interested in are in general not semisimple. In this case, one cannot expect an equivalence of categories: In fact, in the examples discussed below, it may and will happen that A has finite global (cohomological) dimension—so, all extension groups between A-modules vanish in large degrees—while B has infinite global dimension—so, there are non-zero extension groups between B-modules in arbitrarily large degree. The double centraliser property does, however, still provide useful functors relating the representation theories of the algebras A and B.

The best known case of a double centraliser property is that of tensor powers $E^{\otimes r}$ of the natural representation E, typically referred to as (versions of) Schur–Weyl duality. The enveloping algebra in this context is called Schur algebra. We will now state and explain Schur–Weyl duality for the groups considered here.

1.1 Tensor Powers

1.1.1 Classical Schur–Weyl Duality

The n-dimensional k-vector space E is a module for the group $G = \mathrm{GL}_n(k)$, where G acts on E by matrix multiplication. For any natural number r, the group G then acts on the r-fold tensor space $E^{\otimes r}$ by diagonal extension of this action:

$$g \cdot (x_1 \otimes \cdots \otimes x_r) := gx_1 \otimes \ldots gx_r$$

for vectors $x_i \in E$. The symmetric group Σ_r acts by place permutation on the r-fold tensor space. The two actions commute and do, in fact, centralise each other. When

$n \geq r$, the symmetric group acts faithfully with

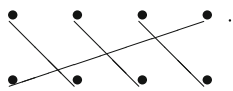
$$\mathrm{End}_{kG}(E^{\otimes r}) = k\Sigma_r \text{ and } \mathrm{End}_{k\Sigma_r}(E^{\otimes r}) = S_{env}(G),$$

where the enveloping algebra $S_{env}(G)$ of G in $\mathrm{End}_k(E^{\otimes r})$ is isomorphic to Green's classical (type A) *Schur algebra* $S(n, r)$. The relevance of Schur algebras is that the category of polynomial G-modules, which are homogenous of degree r, is equivalent to the category of $S(n, r)$-modules. When $n < r$ the above action is no longer faithful and hence the group algebra $k\Sigma_r$ has to be replaced by a certain known quotient algebra. In characteristic zero, classical Schur–Weyl duality is due to Schur [38], in general it follows from results of Carter and Lusztig [4], De Concini and Procesi [7] and Green [22, Theorem 2.6c], and [31], using the connection between double centraliser properties and dominant dimension.

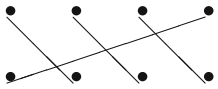
1.1.2 Orthogonal and Symplectic Schur–Weyl Dualities

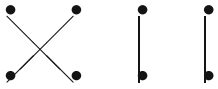
When we replace the general linear group by an orthogonal or symplectic subgroup, the endomorphism ring of tensor space must increase.

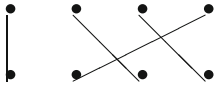
The Brauer Algebra Before describing the endomorphism ring of tensor space in this situation, recall a diagrammatic description of symmetric group elements: Elements of the symmetric group Σ_r on r letters can be visualised by *diagrams*. The following picture shows two ways to write a permutation:

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ corresponds to 

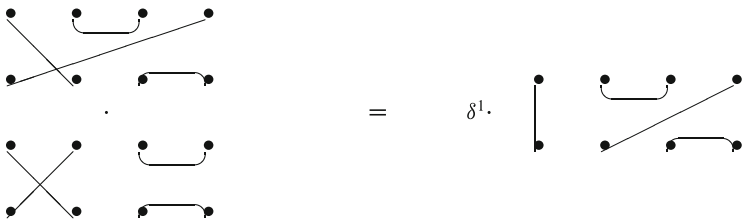
The product of two permutations can be written as concatenation of two diagrams where the vertices of the bottom row of the first diagram are connected vertically with the vertices of the top row of the second diagram:

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ 

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ 

$\pi \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ 

In orthogonal and symplectic Schur–Weyl duality, *Brauer algebras* take the role played by the group algebra of the symmetric group in classical Schur–Weyl duality, described in Sect. 1.1.1. Let k be a field (or any commutative domain), and choose a parameter $\delta \in k$. Let r be a natural number. The Brauer algebra $B_r(\delta)$ of degree r and parameter δ is defined to be the vector space with k-basis given by the set of all Brauer diagrams on $2r$ vertices. A Brauer diagram is a diagram whose vertices are arranged in two rows of r vertices each, and there are r edges between the vertices such that each vertex is incident to precisely one edge. Brauer diagrams are considered up to homotopy, thus the dimension of $B_r(\delta)$ is $(2r-1)!! = (2r-1)\cdot(2r-3)\cdots 3\cdot 1$. To multiply two Brauer diagrams, say b_1 and b_2, the diagrams are concatenated as described for symmetric group elements, with b_1 drawn on top of b_2, and any closed loops appearing are removed, to give a Brauer diagram d. The result of the multiplication then is, by definition, $b_1 \cdot b_2 = \delta^c d$, where c is the number of closed loops removed. Here is an example, the product of two elements in $B_4(\delta)$:



Typically the parameter δ is understood from the context, and we will denote the Brauer algebra by B_r or just B. Brauer algebras were introduced in [2] in the context of generalising Schur–Weyl duality from general linear groups to orthogonal and symplectic subgroups. For more details and examples see, for instance, [2, 3, 23–25, 29, 30, 32]. The restriction of the parameter $\delta = \pm n$ is necessary to obtain an action of the Brauer algebra $B_r(\delta)$ on the r-fold tensor space and on the generalised exterior powers $\wedge^\lambda E$ as well as on the generalised symmetric powers $\mathrm{Sym}^\lambda E$ to be studied below. In characteristic zero, Brauer algebras are semisimple for non-integral parameter and for large integral parameter δ, by a famous result of Wenzl [41].

Orthogonal and Symplectic Groups As before, k is an algebraically closed field of characteristic $p \geq 0$ and let n, r be positive integers. Let E be an n-dimensional k-vector space and let ω be a non-degenerate symmetric bilinear form on E. The orthogonal group relative to ω is

$$\mathrm{O}_n = \{g \in \mathrm{GL}_n \mid \omega(gx, gy) = \omega(x, y) \text{ for all } x, y \in E\}.$$

Similarly for $n = 2m$ even positive integer, let ω be a non-degenerate skew-symmetric bilinear form on E. The symplectic group relative to ω is

$$\mathrm{Sp}_n = \{g \in \mathrm{GL}_n \mid \omega(gx, gy) = \omega(x, y) \text{ for all } x, y \in E\}.$$

All matrices here are defined over the field k, that is $\mathrm{GL}_n = \mathrm{GL}_n(k)$, and so on. The classical groups GL_n, Sp_n and O_n operate on E by matrix multiplication. This action extends diagonally to an action on the tensor space $E^{\otimes r}$, which is connected to Brauer algebras.

The Connection with Brauer Algebras Let $G \in \{\mathrm{Sp}_n, \mathrm{O}_n\}$. Brauer diagrams can be interpreted as G-homomorphisms in the following way: Assume E has basis $\{e_1, \ldots, e_n\}$, and let $\{e^1, \ldots, e^n\}$ be the dual basis of E with respect to the invariant form ω. Define

$$\vartheta = \sum_{i=1}^{n} e_i \otimes e^i.$$

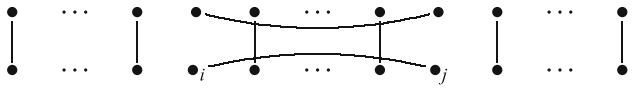
Then ϑ is G-invariant (see [20, 4.3.2.]). For $1 \leq i,j \leq n$, define the (i,j)th contraction operator $C_{i,j} : E^{\otimes r} \to E^{\otimes r-2}$ by

$$C_{i,j}(x_1 \otimes \cdots \otimes x_r) = \omega(x_i, x_j)\, x_1 \otimes \cdots \otimes \hat{x}_i \otimes \cdots \otimes \hat{x}_j \otimes \cdots \otimes x_r$$

with vectors x_i's in E and where we omit the ith vector x_i and the jth vector x_j in the tensor product. Moreover, the (i,j)th expansion operator $D_{i,j} : E^{\otimes r-2} \to E^{\otimes r}$ is defined by

$$D_{i,j}(x_1 \otimes \cdots \otimes x_{r-2}) = \sum_{t=1}^{n} x_1 \otimes \cdots \otimes e_t \otimes \cdots \otimes e^t \otimes \cdots \otimes x_{r-2}.$$

Here e_t is in the ith position and e^t is in the jth position. Setting $b_{ij} = D_{i,j} \circ C_{i,j}$, it is easily checked that $b_{i,j} = b_{j,i}$. It turns out that all elements in $\mathrm{End}_G(E^{\otimes r})$ coincide with elements in the Brauer algebra B_r. When labeling the vertices in the top row as well as the bottom row from left to right by 1 up to r, the element $b_{i,j}$ coincides with the Brauer diagram

$b_{i,j} =$ 

with the horizontal edges between vertices i and j. When considering the action of Brauer algebras on tensor space, the top row horizontal arc corresponds to the contraction operator, and the arc in the bottom row corresponds to the expansion operator.

Diagrams consisting of $r-2l$ through strings connecting top and bottom vertices (and l arcs at corresponding top and bottom places) naturally correspond to elements of a symmetric group Σ_{r-2l}. Such elements are G-endomorphisms of tensor space factoring through the smaller tensor space $E^{\otimes r-2l}$. Every Brauer diagram can be factorised as a product of contraction operators, an element of a symmetric group

Σ_{r-2l} and then a product of expansion operators. This factorisation is the basic ingredient of the cellular structure of the Brauer algebra, for details see [30].

From now on, we assume $n \geq 2r$ in case G is a symplectic group and $n > 2r$ in the orthogonal case. Then the Brauer algebra with parameter $\pm n$ acts faithfully on tensor space $E^{\otimes r}$. Results by Brauer [2] in characteristic zero and in general by De Concini–Procesi [7], Oehms [35], Dipper–Doty–Hu [8, 17] and Tange [40] extend classical Schur–Weyl duality to orthogonal and symplectic subgroups, implying in particular the following two isomorphisms:

$$B_r(n) = \mathrm{End}_{O_n}(E^{\otimes r}), \qquad B_r(-n) = \mathrm{End}_{Sp_n}(E^{\otimes r}). \tag{1.1}$$

$$S_{env}(\mathrm{O}_n) = \mathrm{End}_{B_r(n)}(E^{\otimes r}), \qquad S_{env}(\mathrm{Sp}_n) = \mathrm{End}_{B_r(-n)}(E^{\otimes r}). \tag{1.2}$$

Recall that here $S_{env}(G)$ denotes the enveloping algebra in $\mathrm{End}_k(E^{\otimes r})$ of the respective group (see [16], [33] and [34] for more information on these algebras). A version of Schur–Weyl duality involving $\mathrm{Hom}_G(E^{\otimes s}, E^{\otimes t})$ with s and t not necessarily equal can be found in [40]: In this version, tensor space $E^{\otimes r}$ is replaced by a direct sum $\oplus_{s=0}^{r} E^{\otimes s}$. In [40, Theorem 3], Schur–Weyl duality is shown for this situation; the statement and the conditions in this situation coincide with those of usual Schur–Weyl duality. (This also works in the orthogonal case, see [40, Remark 3].) Here, basis elements of G-homomorphisms between tensor spaces of different degrees are represented by generalised Brauer diagrams (called (u, v)-diagrams in [40]) with u vertices in the top row and v vertices in the bottom row. See [40, Sect. 3] for explanations and details.

1.2 Exterior Powers

Keep the group G as above, let E be its natural representation and $j \leq \dim_k(E)$. The exterior powers $\wedge^j E$ of E are G-representations too, and so are tensor powers of these. For a natural number r, let $\lambda = (\lambda_1, \ldots, \lambda_n)$ be a partition of r (written $\lambda \vdash r$), that is $\lambda_1 \geq \cdots \geq \lambda_n > 0$ and $r = \sum_{i=1}^{n} \lambda_i$ is the sum of all the parts λ_i. (The ordering condition on the parts λ_i is not really important in our context. We may as well use compositions λ, which are unordered partitions of r, denoted by $\lambda \models r$.) Then $\wedge^\lambda E := \wedge^{\lambda_1} E \otimes \cdots \otimes \wedge^{\lambda_n} E$ is a G-representation, where again $g \in G$ is acting diagonally on each entry of the tensor.

1.2.1 The Classical Case of the General Linear Group

Let $n \geq r$ and $G = \mathrm{GL}_n$. Then $\oplus_{\lambda \vdash r} \wedge^\lambda E$ is a faithful representation of the classical Schur algebra $S(n, r)$. Donkin [13], see also [14, 15], has shown that there is a double centraliser property relating $S(n, r)$ and the endomorphism ring $\mathrm{End}_G(\oplus_{\lambda \vdash r} \wedge^\lambda E)$. This endomorphism ring turns out to be Morita equivalent

to $S(n,r)$ itself; when choosing suitable multiplicities of indecomposable direct summands, the two algebras even are isomorphic. This result, which has found plenty of applications in representation theory and invariant theory, relies on a deep structural property of these exterior powers, discovered by Donkin: These modules are tilting modules of $S(n,r)$; more precisely, these are the *characteristic tilting modules* (in the sense of Ringel [36]) of the quasi-hereditary algebras $S(n,r)$. (See Sect. 3 for more information on quasi-hereditary algebras.)

Tilting theory in general is a far reaching generalisation of the theory of Morita equivalences. It provides equivalences not of module categories, but of derived module categories. Derived module categories are much coarser invariants than module categories, and thus there are many more derived equivalences than Morita equivalences. On any tilting module there is a double centraliser property. The functors providing the derived equivalences are constructed from particular modules, called tilting modules, which satisfy strong homological properties and which generalise the projective generators used in Morita theory. Building on work of Auslander and Reiten, Ringel constructed for any quasi-hereditary algebra—and Schur algebras are examples of quasi-hereditary algebras—a particular tilting module, namely the characteristic one. He showed that the endomorphism ring of such a characteristic tilting module again is quasi-hereditary. This endomorphism ring nowadays is called the Ringel dual of the original algebra. Donkin's result then is that Schur algebras $S(n,r)$ for $n \geq r$ are Ringel self-dual. For $n < r$, the Ringel dual may be different, see, for example, [18], but Donkin showed that it is always a quasi-hereditary quotient of some Schur algebra.

1.2.2 The Orthogonal and Symplectic Cases

If G is orthogonal or symplectic, there are partial results by Adamowitch and Rybnikov [1] about characteristic tilting modules and Ringel duality, extending Donkin's results. A full description is, however, still missing.

1.3 Symmetric Powers

The least known case in the orthogonal and symplectic case has been that of tensor powers of symmetric powers.

1.3.1 The Classical Case of General Linear Groups

The classical Schur algebra $S(n,r)$ is dual to the coalgebra of polynomials in n^2 variables and of degree r, which is a subcoalgebra of the regular functions on the general linear groups, see [22]. Therefore, the generalised symmetric powers are injective modules over the classical Schur algebra, which is the endomorphism

ring of a direct sum of injective modules. Thus, nothing new is happening in this situation. This coincidence does, however, not carry over to the other two cases.

1.3.2 The Orthogonal and Symplectic Cases

Until recently, no endomorphism rings of generalised symmetric powers over symplectic or orthogonal groups had been calculated. When studying another, different kind of Schur algebras, which we call *Schur algebras of Brauer algebras* or just *Brauer Schur algebras*, denoted $S_B(n, r)$, it surprisingly turned out that the previously unknown endomorphism algebras of generalised symmetric powers are examples of these. We state the result:

Theorem 1.1 ([28]) *Let $G \subset GL_n$ be an orthogonal or symplectic group, over an algebraically closed field k. Assume $n \geq 2r$ when G is a symplectic group, and $n > 2r$ when G is an orthogonal group. Denote by $B_r = B_r(\delta)$ the Brauer algebra with parameter $\delta = -n \in k$ when G is a symplectic group, and $\delta = n \in k$ when G is an orthogonal group. Then the centraliser algebra*

$$\mathrm{End}_G\Big(\bigoplus_{\lambda \vdash r-2l, 0 \leq l \leq \frac{r}{2}} \mathrm{Sym}^\lambda E\Big)$$

is isomorphic to the Schur algebra $S_B(n, r)$ of the Brauer algebra B_r.

In the following sections, the original approach to Brauer Schur algebras $S_B(n, r)$ will be explained and motivated, and their properties will be described. To conclude this section, we summarise the results and list the endomorphism rings $\mathrm{End} := \mathrm{End}_G(M)$ when known where $G \in \{\mathrm{GL}_n, \mathrm{O}_n, \mathrm{Sp}_n\}$ and M is the tensor space or generalised symmetric or exterior powers:

	Tensor space	Exterior power	Symmetric power
General linear group, $n \geq r$	Schur–Weyl duality $\mathrm{End} = k\Sigma_r$	Tilting theory $\mathrm{End} = S(n, r)$	Schur–Weyl duality
General linear group, $n < r$	Schur–Weyl duality End = quotient of $k\Sigma_r$	Tilting theory End = quotient of a Schur algebra	Schur–Weyl duality
Orthogonal/symplectic group, $n \geq 2r$	Schur–Weyl duality $\mathrm{End} = B_r(\pm n)$	?	$\mathrm{End} = S_B(n, r, \pm n)$ Brauer Schur algebra
Orthogonal/symplectic group, $n < 2r$	Schur–Weyl duality	?	?

2 The Other Side of Schur–Weyl Duality

2.1 The Case of the General Linear Groups and Symmetric Groups

Schur–Weyl duality relates representation theory of infinite general linear groups with representation theory of finite symmetric groups. The bimodule affording the double centraliser property, the tensor space, is a natural choice of a representation of the general linear group, being a tensor product of the natural representation. In order to explain the relevance of tensor space as a representation of the symmetric group, we first consider permutation representations of finite groups.

2.1.1 Permutation Modules of Symmetric Groups

The symmetric group Σ_r on r letters acts on a set X with r elements by permuting these elements. Choosing a vector space with basis X, one obtains a representation of Σ_r given by $r \times r$-permutation matrices, whose entries are zero or one with exactly one entry one in each row and in each column. Such a module is called a permutation representation. Any finite group G is a subgroup of some symmetric group Σ_r and, by restriction of the action, the group G also has a permutation representation. More generally, many representations can be obtained by letting G act on a finite set. This action may not be transitive, that is, X may be a non-trivial disjoint union of many orbits, and it may not be faithful, that is, elements in X may have non-trivial stabilisers. An algebraic construction producing transitive permutation modules goes as follows: Choose a subgroup $H \subset G$ and a field k. View k as the trivial representation of H, with all $h \in H$ acting as multiplication by one. Induce up this representation from H to G by forming the tensor product $\mathrm{ind}_{kH}^{kG} k = k \otimes_{kH} kG$. The resulting vector space is a representation of G, with the group G acting by right multiplication on the vector space $\mathrm{ind}_{kH}^{kG} k$. Its basis is given by the set of cosets $X = H\backslash G$, and the stabiliser subgroup of the coset H is H itself. Using H the trivial group, we find the group algebra kG as an example of such a permutation module.

For the symmetric group $G = \Sigma_r$, a special class of subgroups is especially interesting, the *Young subgroups*: Fix a partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of r (or a composition) and define the Young subgroup $H = \Sigma_{\lambda_1} \times \cdots \times \Sigma_{\lambda_n}$ of G, which is a product of smaller symmetric groups acting on the sets $X_1 = \{1, \ldots, \lambda_1\}$, $X_2 = \{\lambda_1 + 1, \ldots, \lambda_1 + \lambda_2\}$, and so on. The induced module $\mathrm{ind}_{kH}^{kG} k = k \otimes_{k\Sigma_\lambda} k\Sigma_r$ then is denoted by M^λ, with a basis of M^λ given by the set of cosets $\Sigma_\lambda \backslash \Sigma_r$. These are the permutation modules of interest in our context.

In fact, taking $e_1, \ldots, e_n$ as basis of E, the r-fold tensor space of E has a basis consisting of all possible tensors $e_{i_1} \otimes \cdots \otimes e_{i_r}$ with e_{i_j} in the given basis of E, for $1 \leq j \leq r$. The action of Σ_r permutes these tensors, which means that Σ_r acts on the set X of tensors. What are the transitive components, that is the direct summands

of the corresponding representation? Write $i = (i_1, \ldots, i_r)$. Let λ_1 be the number of 1s occuring as indices i_j in $e_i := e_{i_1} \otimes \cdots \otimes e_{i_r}$, let λ_2 be the number of 2s, and so on. Then $\lambda(i) := \lambda = (\lambda_1, \ldots, \lambda_n)$ is a composition of r, called the composition associated with the multi-index $i = (i_1, \ldots, i_r)$. Permuting the entries of e_i does not change the indices occuring in e_i, and every permutation is possible. Thus the stabiliser of $e_{i_1} \otimes \cdots \otimes e_{i_r}$ is the Young subgroup Σ_λ. Therefore, the Σ_r-orbit of e_i corresponds to a representation that is isomorphic to the permutation representation M^λ. To summarise, as a representation of Σ_r, the r-fold tensor space is isomorphic to a direct sum of permutation representations M^λ, with some multiplicities. When $n \geq r$, all partitions λ of r do occur in this decomposition of the tensor space.

2.1.2 Specht Filtered Modules

Permutation modules are not only combinatorially nice to handle but they also have an important structural property in the category of Σ_r-modules. To explain this property, we need to look at the ring structure of the group algebra $k\Sigma_r$. While the Schur algebra $S(n, r)$ introduced in Sect. 1.1.1 is a quasi-hereditary algebra, the group algebra $k\Sigma_r$ is not, unless it is semisimple. But it can be written as $k\Sigma_r = eS(r, r)e$ for some idempotent $e = e^2$ in the Schur algebra $S(r, r)$, that is with both parameters equal to r. As a consequence, $k\Sigma_r$ is a cellular algebra, as defined by Graham and Lehrer [21]. The analogue of Weyl modules, that is of the standard modules of the quasi-hereditary structure, of general linear groups are the Specht modules of symmetric groups. The Specht modules S^λ are indexed by partitions of r. In characteristic zero, the Specht modules are exactly the simple modules, up to isomorphism. In prime characteristic, they are in general not (semi)-simple, but all simple modules occur as quotients of Specht modules. Specht modules can be constructed in a combinatorial way, and as such they exist in each characteristic. The Schur functor $e : S(r, r) - mod \to k\Sigma_r - mod, M \mapsto M \cdot e$, that is given by right multiplication by a certain idempotent e, sends the Weyl modules precisely to the Specht modules (which in the literature sometimes are called dual Specht modules). Let us denote by $\mathcal{F}(Weyl)$ the category of $S(r, r)$-modules having a Weyl filtration, that is, a finite chain of submodules with subquotients being Weyl modules; similarly, we denote by $\mathcal{F}(Specht)$ the category of $k\Sigma_r$-modules having a Specht filtration. The Schur functor restricts to a functor $\mathcal{F}(Weyl) \to \mathcal{F}(Specht)$, or in the language of quasi-hereditary algebras and cellular algebras to a functor $\mathcal{F}(standard) \to \mathcal{F}(cell)$. In characteristic zero (or bigger than r), $\mathcal{F}(Weyl)$ is the category of all $S(r, r)$-modules, $\mathcal{F}(Specht)$ is the category of all $k\Sigma_r$-modules and the Schur functor is an equivalence between these two categories. This equivalence is, in modern terms, the main result of Schur's thesis, who showed in 1901 that in characteristic zero, the representation theories of the general linear and of the finite symmetric group are controlled by the same combinatorics. In 1927, he rederived this equivalence of categories in terms of Schur–Weyl duality, which in his case is a relation between two semisimple algebras (both acting faithfully on tensor space, when $n \geq r$), as discussed in the previous section.

In prime characteristic $2 \leq char(k) \leq r$, the filtered categories $\mathcal{F}(Weyl)$ and $\mathcal{F}(Specht)$ are proper subcategories of the module categories $S(r,r)-mod$ and Σ_r-mod, respectively, which—as remarked above—cannot be equivalent categories. An influential result by Hemmer and Nakano [26] does, however, imply that the filtered categories are equivalent in this situation, as exact categories—except in the case of characteristic two or three; in characteristic three, there is no equivalence of exact categories, and in characteristic two, there is no equivalence at all—this can already be seen by trying the smallest possible example, $k\Sigma_2$ with k of characteristic two.

2.1.3 Projective Objects in Filtered Categories

The projective modules of the Schur algebra are objects in the filtered category $\mathcal{F}(Weyl)$, and they are, of course, projective in this category as well. Thus, their images under the Hemmer–Nakano equivalence must be a full set of projective objects in the filtered category $\mathcal{F}(Specht)$. The projective $k\Sigma_r$-modules do have Specht filtrations (this is one ingredient in the cellular structure of $k\Sigma_r$). So, they are projective objects in the category $\mathcal{F}(Specht)$. But they do not form a full set of projective objects there. It turns out that the full set of projective objects in $\mathcal{F}(Specht)$ are provided by the permutation modules M^λ, which are in fact the images of the projective $S(r,r)$-modules under the Schur functor; moreover, $eS(r,r)$ is just tensor space. This is their structural property announced above. In particular, a structural reason for tensor space occurring in our context is that it is a full sum of indecomposable projective objects in $\mathcal{F}(Specht)$. Here full means that each isomorphism type occurs at least once. Such projective objects in subcategories often are called *relative projective modules*.

2.2 *The Case of the Orthogonal and Symplectic Groups and Brauer Algebras*

When trying to find in this case analogies to the objects and their relations described above, there are some surprises. As before, Schur–Weyl duality relates representation theory of symplectic and orthogonal subgroups of the general linear groups with representation theory of Brauer algebras. As before, the Brauer algebra is a cellular algebra. Thus the category $\mathcal{F}(Specht)$ still exists, where the term Specht module refers to the cell modules of the cellular structure of the Brauer algebra (see [21]). However, tensor space is, in general, not Specht filtered (see [29]); thus it has been a problem to find 'permutation modules' that are relative projective in the category of Specht filtered modules. Moreover, an analogue of the Hemmer–Nakano theorem had to be found.

2.2.1 Permutation Modules of Brauer Algebras

Is there an analogue of permutation modules, and are these the projective objects in $\mathcal{F}(Specht)$? This last question has been answered by Hartmann and Paget [24]: here again the theory works in full analogy to the cellular structure of the group algebra of the symmetric group, and works as follows: For $l \leq \frac{r}{2}$ and $\lambda \vdash r-2l$, the permutation module $M(l,\lambda)$ is defined as

$$M(l,\lambda) = M^{\lambda} \otimes_{k\Sigma_{r-2l}} e_l B_r$$

where

$e_l = \frac{1}{\delta^l} \cdot$ (2.1)

with l arcs in the top and bottom row of the diagram, respectively, and M^{λ} is the permutation module (indexed by λ) associated with the symmetric group Σ_{r-2l}. It should be noted that both the basis vectors of tensor space and the idempotents of the Brauer algebra are denoted in the literature by the symbol e_i; the meaning will be clear from the context.

Hartmann and Paget showed by combinatorial methods that these permutation modules $M(l,\lambda)$ in fact are the projective objects in the filtered category $\mathcal{F}(Specht)$. A more structural and much more general approach has been developed in [25], based on the concept of cellularly stratified algebras introduced there.

2.2.2 Two Different Types of Schur Algebras and Their Schur–Weyl Dualities

In type A, the classical situation, tensor space is Weyl filtered when seen over the general linear group; and tensor space is Specht filtered and a direct sum of permutation modules M^{λ} when seen over the group algebra of the symmetric group. By Sect. 2.1.1, the classical Schur algebra

$$\mathrm{End}_{k\Sigma_r}(E^{\otimes r}) = S(n,r) = \mathrm{End}_{k\Sigma_r}(\bigoplus_{\lambda \vDash r} M^{\lambda})$$

is the endomorphism ring of tensor space, but equally well, the endomorphism ring of a full sum of permutation modules. For orthogonal and symplectic groups G, tensor space is Weyl filtered over the orthogonal and symplectic groups. But here is now a fundamental difference: Tensor space is in general not Specht filtered and hence not a direct sum of permutation modules over the Brauer algebra, for details, see [29]. We therefore have two different algebras, taking the place of the classical Schur algebra: the first algebra is Donkin's [12] generalised Schur algebra, also

referred to as symplectic or orthogonal Schur algebra:

$$S_{env}(G) := \mathrm{End}_{B_r}(E^{\otimes r}).$$

The second algebra, the Brauer Schur algebra, is defined to be the endomorphism ring of a full (meaning each isomorphism type occurs at least once) direct sum of all the permutation modules $M(l, \lambda)$, possibly with appropriately chosen multiplicities:

$$S_B(n, r, \delta) = S_B(n, r) = \mathrm{End}_{B_r}\Big(\bigoplus_{\lambda \vdash r-2l, 0 \le l \le \frac{r}{2}} M(l, \lambda)\Big).$$

The Brauer Schur algebra is, in general, not isomorphic to the Schur algebra of the orthogonal or symplectic group, and it is defined much more generally. One of its relevances is that the Brauer Schur algebra is the endomorphism ring of the direct sum of tensor powers of symmetric powers, see Theorem 1.1, with appropriate parameter δ.

Together with these two different types of Schur algebras come two different Schur–Weyl dualities for the Brauer algebra: There is a Schur–Weyl duality on tensor space, relating Donkin's generalised Schur algebra with the Brauer algebra, as described in Sect. 1.1.2. However, there is also a Schur–Weyl duality (observed abstractly in [25] and combinatorially in [27]) on the full direct sum of the permutation modules $M(l, \lambda)$, relating the Brauer Schur algebra with the Brauer algebra. More of this will be described in the next section.

3 Properties of Brauer Schur Algebras

In the final section of the article we summarise the ring theoretical and homological properties of Brauer Schur algebras. To do so, we first have another look at the classical Schur algebra, which has been defined as

$$S(n, r) = \mathrm{End}_{k\Sigma_r}(E^{\otimes r}) = \mathrm{End}_{k\Sigma_r}(\oplus M^{\lambda})$$

where the sum runs over all compositions of r with at most n parts.

3.1 Combinatorial Bases of Schur Algebras of Brauer Algebras

In order to work with such an algebra, a more explicit definition is useful, given by a basis and a multiplication formula. Denote by $I(n, r)$ the set of multi-indices of length r with entries in the set $\{1, \ldots, n\}$. The symmetric group Σ_r operates on the set of multi-indices $I(n, r)$ by permuting places, and hence the stabiliser of a multi-index is defined, $\mathrm{Stab}(i) = \{\tau \in \Sigma_r \mid i\tau = i\}$. Recall the definition of a composition

$\lambda(i)$ associated with a given multi-index i, given in Sect. 2.1.1. One of the standardly used bases of the classical Schur algebra is indexed by certain pairs of multi-indices: Let $k, l \in I(n, r)$ with associated compositions $\lambda(k) = \mu$ and $\lambda(l) = \lambda$, respectively. Define the Σ_r-homomorphism $\xi_{k,l} : M^\lambda \to M^\mu$ on the generator e_l (or alternatively on the coset generator $\Sigma_\lambda \cdot \mathrm{id}$) of the Σ_r-module M^λ by

$$\xi_{k,l}(\Sigma_\lambda \cdot \mathrm{id}) = \xi_{k,l}(e_l) = \sum_{i \in I(n,r)} \xi_{k,l}(c_{i,l}) e_i. \tag{3.1}$$

Here the scalar $\xi_{k,l}(c_{i,l}) = 0$ unless there exists a permutation $\pi \in \mathrm{Stab}(l)$ with $k\pi = i$ in which case we define $\xi_{k,l}(c_{i,l}) = 1$. This definition is extended such that we have an equality of maps $\xi_{i,j} = \xi_{k,l}$ if and only if there is a permutation $\pi \in \Sigma_r$ which simultaneously permutes i into k and j into l. The set of all such homomorphisms is an integral basis of the classical Schur algebra. This basis is defined in combinatorial terms only, and hence is independent of the ground field and its characteristics. There is a nice, but combinatorially involved, multiplication formula for two such basis vectors, expressing the product again as a linear combination in this basis. The structure constants here are given by the cardinality of certain sets, and hence are non-negative integers, and in particular, multiplication will depend on the characteristic of the underlying field, but the multiplication rule as such does not depend and the combinatorial description of the basis doesn't either. This is a characteristic free property in the sense of the aims stated in the introduction.

The precise multiplication rule is as follows (see [22, (2.3b)]):

$$\xi_{i,j} \cdot \xi_{k,l} = \sum_{(p,q)} Z(i, j, k, l, p, q) \xi_{p,q}$$

where the sum is over a set of representatives (p, q) of orbits of the symmetric group Σ_r acting on $I(n, r) \times I(n, r)$. The number $Z(i, j, k, l, p, q)$—to be seen as an element of the ground field—counts $s \in I(n, r)$ such that (i, j) and (p, s) are in the same Σ_r-orbit and also (k, l) and (s, q) are in the same orbit. Thus, the product is zero if j and k are not in the same Σ_r-orbit.

We rewrite the homomorphisms given in (3.1). For a composition λ, write $\mathrm{ind}(\lambda)$ for a multi-index i whose entries are ordered increasingly with associated composition λ. By the definition of the scalars in (3.1), without loss of generality, we may assume in the above setup that the entries of the multi-index l are ordered increasingly, that is, $l = \mathrm{ind}(\lambda)$. There exists a permutation σ with $k = \mathrm{ind}(\mu)\sigma$, and hence

$$\mathrm{Stab}(l) \cap \mathrm{Stab}(k) = \Sigma_\lambda \cap \sigma^{-1} \Sigma_\mu \sigma.$$

The sum in (3.1) can thus be rewritten by

$$\xi_{k,l}(\Sigma_\lambda \cdot \mathrm{id}) = \xi_{k,l}(e_l) = \sum_{\alpha \in (\Sigma_\lambda \cap \sigma^{-1}\Sigma_\mu \sigma)\backslash \Sigma_\lambda} e_{\mathrm{ind}(\mu)} \sigma \alpha.$$

We now look at the Brauer Schur algebra. For any fixed parameter $\delta \neq 0$ in the field k, the Brauer Schur algebra is

$$S_B(n,r) = \mathrm{End}_{B_r}\Big(\bigoplus_{\lambda \vdash r-2l, 0 \leq l \leq \frac{r}{2}} M(l,\lambda)\Big).$$

In analogy to the above basis of the classical Schur algebra, an explicit integral basis of the Brauer Schur algebra $S_B(n,r)$, indexed by certain double cosets, has been constructed in [27, Theorem 5.3]. Let λ be a partition of $r-2l$ and μ a partition of $r-2m$ and let $u \geq l, m$. For a natural number s define the group $H_s = C_2 \wr \Sigma_s$. Choose representatives π and σ of the double cosets $\Sigma_\mu \backslash \Sigma_{r-2m} / (\Sigma_{r-2u} \times H_{u-m})$ and $(\Sigma_\nu \times H_{u-l}) \backslash \Sigma_{r-2l} / \Sigma_\lambda$, respectively, where $\Sigma_\nu = \Sigma_{r-2u} \cap \pi^{-1}\Sigma_\mu \pi$. Define the B-homomorphism $\phi_{u,\pi,\sigma} : M(l,\lambda) \to M(m,\mu)$ on a generator by:

$$\phi_{u,\pi,\sigma}(\Sigma_\lambda \cdot id \otimes e_l) = \sum_{\alpha \in \Sigma_\lambda \cap \sigma^{-1}(\Sigma_\nu \times H_{u-l})\sigma \backslash \Sigma_\lambda} (\Sigma_\mu \cdot id \otimes e_{\pi,u})\sigma \cdot \alpha.$$

Theorem 3.1 ([27, Theorem 7.1]) *The set of all such B-homomorphisms forms a basis of the Brauer Schur algebra $S_B(n,r)$.*

Again this basis itself does depend on various combinatorial data, however, not on the ground field k and its characteristics, nor the parameter δ of the Brauer algebra. So, the Brauer Schur algebra is defined integrally and hence over any ground ring by change of scalars. Products of two such basis vectors can be computed in analogy to the multiplication in the classical Schur algebra, in particular, structure constants are again non-negative integers. This basis is characteristic free in the same way as Green's basis of the classical Schur algebra.

The B-modules $M(l,\lambda)$ are by definition induced from the Σ_r-modules M^λ. Therefore, inducing up a map $M^\lambda \to M^\mu$ yields a map $M(l,\lambda) \to M(l,\mu)$—note that both modules have the same index l. Checking the details of the above description one shows that in this way Green's basis elements $\xi_{i,j}$ correspond to basis elements $\phi_{u,id,\sigma} : M(l,\lambda) \to M(l,\mu)$ where $\lambda = \lambda(j)$ and j has non-decreasing entries, $\mu = \lambda(i)$ and i is obtained from the index with non-decreasing entries by applying the permutation σ. So, the above basis of $S_B(n,r)$ is indeed an extension of Green's basis of the classical Schur algebra $S(n, r-2l)$. Checking the multiplication rules, it turns out that the classical Schur algebra $S(n, r-2l)$ is (for each l) a non-unital subalgebra of $S_B(n,r)$. It follows that the (in general unknown) decomposition matrices of classical Schur algebras are diagonal submatrices of the decomposition matrix of the Brauer Schur algebra $S_B(n,r)$. See Sect. 6 in [27] for details.

3.2 Quasi-Hereditary Structure

Quasi-hereditary algebras were introduced by Scott [39] in the context of highest weight categories. They arise naturally in the representation theory of semisimple complex Lie algebras and algebraic groups. Cline, Parshall and Scott have shown that in general highest weight categories can be described in terms of quasi-hereditary algebras and their module categories, see [5, 6]. Many other algebras have been shown to be quasi-hereditary too, for instance, path algebras of quivers, and more generally algebras of global dimension less than or equal to two.

There are two customary ways to define quasi-hereditary algebras. One is based on the existence of a chain $0 \subset J_1 \subset \cdots \subset J_n = A$ of two-sided ideals, called *heredity chain*. These ideals are required to be generated by idempotent elements and to satisfy strong homological conditions, which, for instance, imply that the derived module category of the algebra A contains the derived categories of the quotient algebras A/J_l (for each l) as full subcategories. In particular, cohomology between A/J_l-modules coincides with cohomology of the same modules viewed as A-modules.

The other definition is based on the existence of a collection of modules, called *standard modules*, $\Delta_1, \ldots, \Delta_n$. Homomorphisms and extensions between these modules are allowed only in increasing order; $\mathrm{Hom}(\Delta_i, \Delta_j) \neq 0$ implies $i \leq j$ and $\mathrm{Ext}^1(\Delta_i, \Delta_j) \neq 0$ implies $i < j$. Moreover, their endomorphism rings are skew-fields and their composition factors also satisfy an ordering condition. Such standard modules occur in nature as Weyl modules of algebraic groups, as Verma modules of semisimple complex Lie algebra or as exceptional coherent sheaves. By Dlab and Ringel's 'standardisation theorem' [11], behind every set of standard objects (in an abelian category) there is a quasi-hereditary algebra. Therefore, quasi-hereditary algebras are being studied in many areas, from representation theory over Lie theory to algebraic geometry.

Donkin [12] showed that generalised Schur algebras are quasi-hereditary algebras. What about Brauer Schur algebras? As explained above, analysing certain subsets $\mathcal{B}_l$ with $0 \leq l \leq r/2$ of the above basis of the Brauer Schur algebra and their multiplication, one can show that the vector space spanned by $\mathcal{B}_l$ is isomorphic to a classical (type A) Schur algebras $S(n, r-2l)$, mapping basis vectors in $\mathcal{B}_l$ to the respective $\xi_{i,j}$-basis. Classical Schur algebras are quasi-hereditary, by Donkin's work [12]. Using that the classical Schur algebras $S(n, r-2l)$ can be embedded diagonally into the Brauer Schur algebra as described, it follows together with a characterisation of quasi-hereditary algebras by Dlab and Ringel [10]:

Theorem 3.2 ([27, Theorem 7.1]) *The Brauer Schur algebra $S_B(n, r)$ is a quasi-hereditary algebra.*

Thus the module category of the Brauer Schur algebra is a highest weight category in the sense of Cline, Parshall and Scott. In the proof, a heredity chain of the Brauer Schur algebra is constructed by inducing up the heredity chains of the diagonally embedded classical Schur algebras $S(n, r-2l)$. In particular, the simple

$S_B(n, r)$-modules are parametrised in the same way as the simple modules of all the classical Schur algebras $S(n, r-2l)$ for $0 \leq l \leq r/2$ together, that is by the partitions into at most n parts of $r, r-2, r-4, \ldots, 1$ or 0, depending on whether r is odd or even. The proof also provides a description of the standard modules (the analogue of the Weyl modules) of the Brauer Schur algebra.

Quasi-hereditary algebras also provide the basic setup for Ringel's theory of characteristic tilting modules, which in the case of classical Schur algebras are certain direct sums of tensor powers of exterior powers, as explained in Sect. 1.2.1. Ringel's theory implies that such modules must exist for Brauer Schur algebras as well; a detailed description of these modules is, however, still missing.

Brauer algebras are, in general, not quasi-hereditary. As mentioned already, they carry a weaker structure, being cellular in the sense of Graham and Lehrer [21]. For a detailed discussion of the cellular structure of Brauer algebras, see [30]. Quasi-hereditary algebras A together with a duality (involutory anti-automorphism) preserving the heredity chain are cellular. Moreover, then the algebra eAe is cellular, too, where e is any idempotent fixed by the duality. The cell (Specht) modules of the algebra eAe are just the standard modules of A multiplied by e. In this way, the quasi-hereditary structure of the classical Schur algebra induces a cellular structure on the group algebra of the symmetric group, and the quasi-hereditary structure of the Brauer Schur algebra (but also that of $S_{env}(G)$) induces the cellular structure of the Brauer algebra that has been mentioned above. This provides further relevance for the Schur functors to be discussed in more detail in the final subsection below.

3.3 Homological Properties, Covers and Uniqueness

Next, we discuss homological properties of the Brauer Schur algebra. Given an algebra A, the minimal length of all finite projective resolutions of a given A-module is called its projective dimension. The *global dimension* of an algebra is by definition the supremum of the set of projective dimensions of all A-modules. Thus the global dimension is either a natural number or infinity. The algebra A has finite global dimension, say d if and only if there is non-vanishing cohomology between some A- modules in degrees $0, 1, \ldots, d$, but from degree $d+1$ all cohomology vanishes. The global dimension is not directly related to representation theory; for instance, there is no correlation with representation type (finite, tame or wild). However, it characterises classes of algebras: An algebra has global dimension zero if and only if it is semisimple; prominent examples of such algebras are group algebras where the characteristic of the underlying field is not dividing the order of the group. An algebra has global dimension less than or equal to one if and only if it is hereditary, that happens if and only if every submodule of a projective module is again projective; prominent examples of such algebras are path algebras of quivers. By Cline, Parshall and Scott [6, Theorem 4.4] and Dlab and Ringel [9, Appendix, Statement 9], all quasi-hereditary algebras have finite global dimension, and hence the Brauer Schur algebra has finite global dimension.

As we have seen, there is a close relationship between the classical Schur algebra $A = S(n, r)$ (for $n \geq r$) and the group algebra $k\Sigma_r$ of the symmetric group on r letters, which is of the form $k\Sigma_r = eAe$ for some idempotent element $e = e^2 \in A$. Multiplication by the idempotent e defines an exact functor sending A-modules to eAe-modules. How strong is the relation provided by this functor, the Schur functor? In [19] it has been shown that another homological dimension, the dominant dimension of A, controls this situation for classical Schur algebras. The double centraliser property (Schur–Weyl duality) can be expressed as saying that the dominant dimension of A is at least two, and the quality of the Schur functor, when comparing cohomology of Weyl and Specht filtered modules, is measured in a precise sense by the dominant dimension of A. Classical dominant dimension requires Ae to be a projective–injective A-module. It is not known when $\oplus M(l, \lambda)$ is projective–injective over the Brauer Schur algebra. Therefore, when trying to find an analogue of the results in [19] for the Brauer Schur algebra, one has to work with a relative dominant dimension, with respect to $\oplus M(l, \lambda)$. The Schur–Weyl duality between the Brauer algebra and its Schur algebra is equivalent to this relative dominant dimension being at least two. The precise value of this relative dominant dimension so far has not yet been determined.

Instead of starting with a given algebra A and asking for its relation with a particular centraliser algebra eAe, we may ask conversely: Given an algebra B, can we find a quasi-hereditary algebra A such that $B \simeq eAe$? Can we even find the best possible A, that is, the one with the strongest connection to B? To investigate such questions, Rouquier [37] introduced the concept of quasi-hereditary covers. This concept is closely related to relative dominant dimension with respect to a projective module that is not required to be injective. More precisely, for a natural number i, an i-cover is defined in order to compare the cohomology up to degree i of modules of certain algebras. A quasi-hereditary algebra A is called a 0-cover of eAe for an idempotent $e \in A$, if A and eAe satisfy a double centraliser property with respect to the bimodule eA. And A is a 1-cover of eAe with respect to the bimodule eA, if in addition, the category $\mathcal{F}_A(\Delta)$ of A-modules with a filtration by standard modules is equivalent via the Schur functor $e \cdot -$ to the category $\mathcal{F}_{eAe}(\Delta e)$ of eAe-modules with a filtration by modules Δe. So, by the result of Hemmer and Nakano, the classical Schur algebra $S(r, r)$ is a quasi-hereditary 1-cover of the group algebra $k\Sigma_r$, provided the characteristic of k is different from two and three. Rouquier showed that 0-covers always exist; he also showed that 1-covers, if they exist, are satisfying a universal property that makes them unique up to Morita equivalence.

Theorem 3.3 ([27, Theorem 11.4(b) and (c)]) *When the characteristic is different from two or three, the Brauer Schur algebra $S_B(n, r)$ is the quasi-hereditary 1-cover of the Brauer algebra B_r, and as such it is uniquely determined up to Morita equivalence.*

In this abstract setup, Brauer Schur algebras have come up for the first time, in [25]; the explicit construction in [27] is more general, since it does not need any assumption on the characteristic.

In the language as explained above, choosing idempotent $e : \oplus M(l, \lambda) \to M(0, (1^r)) = B_r$ in $S_B(n, r)$, the two algebras B_r and $S_B(n, r)$ are in Schur–Weyl duality with respect to the bimodule $e \cdot S_B(n, r) = \oplus M(l, \lambda)$ where the sums always run over all possible permutation modules. By [24], needing the characteristic of the underlying field being different from two and three, we can identify extension spaces between modules with standard filtration over $S_B(n, r)$ with extension spaces over B_r:

$$\mathrm{Ext}^1_{S_B(n,r)}(X, Y) \simeq \mathrm{Ext}^1_{B_r}(eX, eY),$$

which implies that the Brauer Schur algebra is a quasi-hereditary 1-cover of the Brauer algebra B_r. See [25, Sects. 11–13] for explicit statements and for more information.

3.4 A Lie Theoretic Context for Brauer Schur Algebras

We now return to working again in the context of orthogonal and symplectic groups, and hence choose again the parameter δ of the Brauer Schur algebra to be n or $-n$, respectively. Schur–Weyl duality is given by a bimodule, and this in turn gives rise to two functors, the Schur functor and the inverse Schur functor. In the context of the classical Schur algebra, the tensor space is a bimodule for the classical Schur algebra $S(n, r)$ and the group algebra of the symmetric group Σ_r which gives rise to the Schur functors and the inverse Schur functor:

$$\text{mod-}G \supset \text{mod-}S_{env}(G) = \text{mod-}S(n, r) = \text{mod-End}_{\Sigma_r}(E^{\otimes r}) = \text{mod-End}_{\Sigma_r}(\oplus M^\lambda)$$

$$\begin{array}{ccc} & f \downarrow \quad \uparrow g & \\ \text{mod-}k\Sigma_r & & \end{array}$$

with $G = \mathrm{GL}_n(k)$ and functors $f = \mathrm{Hom}_G(E^{\otimes r}, -)$ and $g = - \otimes_{\Sigma_r} E^{\otimes r}$. In case one of the involved algebras is semisimple, for example, when the characteristic of the underlying field is zero, these functors provide the equivalence between $k\Sigma_r$-mod and $S(n, r)$-mod; and otherwise, they provide an exact equivalence between the category of Weyl-filtered $S(n, r)$-modules and the category of cell-filtered $k\Sigma_r$-modules, provided the characteristic of the underlying field is different from two and three. Thus Schur functor and inverse Schur functor are connecting a certain part of the representation theory of general linear groups, with that of symmetric groups, that is, the functors provide a connection between Lie theory and combinatorics.

The above diagram summarises the following results:

- *Classical Schur–Weyl duality states that* $S(n,r) = \mathrm{End}_{\Sigma_r}(E^{\otimes r})$.
- *The Schur functor f and the 'inverse Schur functor' g (which is a one-sided inverse only) relate the representation theories of* $S(n,r)$ *and of* $k\Sigma_r$*, specialising to an equivalence of categories between Weyl and Specht filtered modules (in characteristic different from two and three).*
- *The Schur algebra (defined as endomorphism ring) equals the enveloping algebra* $S_{env}(G)$ *(which is a quotient of the group algebra kG).*
- *Tensor space is a relative projective generator of the category of modules with Specht filtration, and it is a direct sum of permutation modules.*

We consider now the same situation for Brauer Schur algebras. As in types B, C and D, tensor space is different from the sum of permutation modules over B_r, there are now two sets of Schur functors related to this situation, a pair of functors (f_0, g_0) related to the tensor space and a pair of functors (F_M, G_M) related to the full sum of permutation modules:

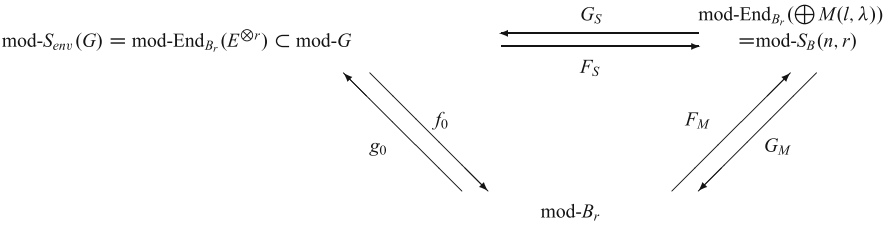
$$\begin{aligned} f_0 &= \mathrm{Hom}_G(E^{\otimes r}, -), & F_M &= \mathrm{Hom}_{B_r}(\oplus M(l,\lambda), -), \\ g_0 &= - \otimes_{B_r} E^{\otimes r}, & G_M &= - \otimes_{S_B(n,r)} (\oplus M(l,\lambda)). \end{aligned}$$

The functors f_0 and g_0 are the Schur functors relating Donkin's orthogonal or symplectic Schur algebra $S_{env}(G)$ with the Brauer algebra. The functors F_M and G_M are the Schur functors relating representation theory of the Brauer Schur algebra with that of the Brauer algebra. By Theorem 1.1, we have $S_B(n,r) \simeq \mathrm{End}_G(\bigoplus_{\lambda \vdash r-2l, 0 \le l \le \frac{r}{2}} \mathrm{Sym}^\lambda E)$. Define in addition functors related to the full sum of symmetric powers:

$$F_S = \mathrm{Hom}_G(\oplus \mathrm{Sym}^\lambda E, -), \qquad G_S = - \otimes_{S_B(n,r)} (\oplus \mathrm{Sym}^\lambda E).$$

These functors relate Donkin's orthogonal and symplectic Schur algebras with the Brauer Schur algebras, when the parameter δ of the Brauer Schur algebras is appropriately specialised.

To summarise, we have the following triangle of functors, relating the representation theory of the two different Schur algebras in the top row with the representation theory of Brauer algebra in the bottom row. In particular, by Theorem 1.1 we have obtained a Lie theoretic context for the representation theory of Brauer Schur algebras:



This triangle commutes in the sense that $G_S = g_0 \circ G_M$ and similarly for the adjoints. Indeed, there are isomorphisms of left $S_B(n,r)$-modules

$$M(l,\lambda) \otimes_{B_r} E^{\otimes r} \simeq M^{\lambda} \otimes_{k\Sigma_{r-2l}} e_l B_r \otimes_{B_r} E^{\otimes r} \simeq \mathrm{Sym}^{\lambda} E \otimes \vartheta^l \simeq \mathrm{Sym}^{\lambda} E.$$

Tensor functor and Hom-functor are adjoint functors. Uniqueness of adjoints then implies $F_S = F_M \circ f_0$. Again, if one of the involved algebras is semisimple, then all involved module categories are equivalent. Of interest is now the question what happens when none of these algebras is semisimple. In analogy to the picture above in type A, when the ground field k has characteristic different from two and three, the functors F_M and G_M are mutually inverse equivalences between the exact categories of Δ-filtered $S_B(n,r)$-modules and cell filtered B_r-modules, by [24]. Thus an analogue of the theorem of Hemmer and Nakano [26] mentioned above holds true. It is not known how well these two functors compare or identify cohomology in higher degrees. Following [19], where the classical type A case has been clarified, this amounts to saying that the dominant dimension of $S_B(n,r)$ relative to $\oplus M(l,\lambda)$ is not known. It is open whether the other two pairs of functors are restricting to equivalences between corresponding categories of filtered modules. Also, the (relative) dominant dimensions of generalised Schur algebras (including the enveloping algebras $S_{env}(G)$) are not known. In other words, it is not known how good the various Schur functors are in comparing cohomology.

The above diagram summarises the following results:

- *There is a Schur–Weyl duality between the enveloping algebra $S_{env}(G)$ and the Brauer algebra B_r. The bimodule affording the Schur–Weyl-duality is tensor space.*
- *There is another Schur–Weyl duality between the Brauer Schur algebra $S_B(n,r)$ and the Brauer algebra B_r. The bimodule is a full direct sum of permutation modules of B_r. These are relative projective in the category of Specht filtered modules, which in general does not contain tensor space.*
- *The enveloping algebra $S_{env}(G)$ and the Brauer Schur algebra $S_B(n,r)$ are in general different algebras.*
- *There is a third Schur–Weyl duality between $S_{env}(G)$ and $S_B(n,r)$. The bimodule is a full direct sum of tensor powers of symmetric powers. In particular, $S_B(n,r)$ is the endomorphism ring over G of this module (Theorem 1.1).*
- *The Schur functor G_M and the 'inverse Schur functor' F_M (which is a one-sided inverse only) provide an equivalence of categories between Weyl and Specht filtered modules (in characteristic different from two and three).*
- *The other two pairs of adjoint functors, (g_0, f_0) and (G_S, F_S), relate the representation theories of the respective algebras, but are not known to specialise to equivalences of subcategories.*

As explained in Sect. 1, the Lie theoretic context provided here is strong enough to solve the classical problem of describing endomorphisms of sums of tensor products of symmetric powers. The precise nature of the connections given by the above triangle of functors remains, however, to be explored.

All of what just has been said refers to the case of Brauer Schur algebras with integer parameters δ in order to have a link to orthogonal or symplectic groups. If the parameter δ is not an integer, the Brauer Schur algebra still is quasi-hereditary and its module category is a highest weight category. No Lie theoretic object is known that can play the role of $S_{env}(G)$ or of G itself in the above triangle of functors.

References

1. A.M. Adamovich, G.L. Rybnikov, Tilting modules for classical groups and Howe duality in positive characteristic. Transform. Groups **1**(1–2), 1–34 (1996)
2. R. Brauer, On algebras which are connected with the semisimple continuous groups. Ann. Math. **38**, 854–872 (1937)
3. W.P. Brown, The semisimplicity of ω_f^n. Ann. Math. (2) **63**, 324–335 (1956)
4. R. Carter, G. Lusztig, On the modular representations of the general linear and symmetric groups. Math. Z. **136**, 193–242 (1974)
5. E. Cline, B. Parshall, L. Scott, Finite-dimensional algebras and highest weight categories. J. Reine Angew. Math. **391**, 85–99 (1988)
6. E. Cline, B. Parshall, L. Scott, Algebraic stratification in representation categories. J. Algebra **117**, 504–521 (1988)
7. C. De Concini, C. Procesi, A characteristic free approach to invariant theory. Adv. Math. **21**(3), 330–354 (1976)
8. R. Dipper, S. Doty, J. Hu, Brauer's centralizer algebras, symplectic Schur algebras, and Schur-Weyl duality. Trans. Am. Math. Soc. **360**, 189–213 (2008)
9. V. Dlab, C.M. Ringel, Quasi-hereditary algebras. Illinois J. Math. **33**, 280–291 (1989)
10. V. Dlab, C.M. Ringel, A construction for quasi-hereditary algebras. Compos. Math. **70**, 155–175 (1989)
11. V. Dlab, C.M. Ringel, The module theoretical approach to quasi-hereditary algebras, in *Representations of Algebras and Related Topics (Kyoto, 1990)*. London Mathematical Society Lecture Note Series, vol. 168 (Cambridge University Press, Cambridge, 1992), pp. 200–224
12. S. Donkin, On Schur algebras and related algebras. I. J. Algebra **104**(2), 310–328 (1986); On Schur algebras and related algebras. II. J. Algebra **111**(2), 354–364 (1987)
13. S. Donkin, On tilting modules for algebraic groups. Math. Z. **212**(1), 39–60 (1993)
14. S. Donkin, On tilting modules and invariants for algebraic groups, in *Finite-Dimensional Algebras and Related Topics (Ottawa, ON, 1992)*. NATO Advanced Science Institutes Series C: Mathematical and Physical Sciences, vol. 424 (Kluwer Academic Publishers, Dordrecht, 1994), pp. 59–77
15. S. Donkin, *The q-Schur Algebra.* London Mathematical Society Lecture Note Series, vol. 253 (Cambridge University Press, Cambridge, 1998), x+179 pp.
16. S. Donkin, R. Tange, The Brauer algebra and the symplectic Schur algebra. Math. Z. **265**, 187–219 (2010)
17. S. Doty, J. Hu, Schur-Weyl duality for orthogonal groups. Proc. Lond. Math. Soc. (3) **98**, 679–713 (2009)
18. K. Erdmann, A. Henke, On Ringel duality for Schur algebras. Math. Proc. Camb. Philos. Soc. **132**, 97–116 (2002)
19. M. Fang, S. Koenig, Schur functors and dominant dimension. Trans. Am. Math. Soc. **363**(3), 1555–1576 (2011)

20. R. Goodman, N. Wallach, Representations and invariants of the classical groups, in *Encyclopedia of Mathematics and Its Applications*, vol. 68 (Cambridge University Press, Cambridge, 1998), xvi+685 pp.
21. J. Graham, G. Lehrer, Cellular algebras. Invent. Math. **123**, 1–34 (1996)
22. J.A. Green, *Polynomial Representations of* GL_n. Lecture Notes in Mathematics, vol. 830 (Springer, Berlin/New York, 1980)
23. P. Hanlon, D. Wales, On the decomposition of Brauer's centralizer algebras. J. Algebra **121**, 409–445 (1989)
24. R. Hartmann, R. Paget, Young modules and filtration multiplicities for Brauer algebras. Math. Z. **254**, 333–357 (2006)
25. R. Hartmann, A. Henke, S. Koenig, R. Paget, Cohomological stratification of diagram algebras. Math. Ann. **347**, 765–804 (2010)
26. D. Hemmer, D. Nakano, Specht filtrations for Hecke algebras of type A. J. Lond. Math. Soc. (2) **69**, 623–638 (2004)
27. A. Henke, S. Koenig, Schur algebras of Brauer algebras, I. Math. Z. **272**(3–4), 729–759 (2012)
28. A. Henke, S. Koenig, Schur algebras of Brauer algebras, II. Math. Z. **276**(3), 1077–1099 (2014)
29. A. Henke, R. Paget, Brauer algebras with parameter $n = 2$ acting on tensor space. Algebr. Represent. Theory **11**(6), 545–575 (2008)
30. S. Koenig, C.C. Xi, A characteristic free approach to Brauer algebras. Trans. Am. Math. Soc. **353**, 1489–1505 (2001)
31. S. Koenig, I.H. Slungard, C.C. Xi, Double centralizer properties, dominant dimension, and tilting modules. J. Algebra **240**, 393–412 (2001)
32. G.I. Lehrer, R.B. Zhang, The Brauer category and invariant theory. J. Eur. Math. Soc. (JEMS) **17**(9), 2311–2351 (2015)
33. Q. Liu, Schur algebras of classical groups. J. Algebra **301**, 867–887 (2006)
34. Q. Liu, Schur algebras of classical groups II. Commun. Algebra **38**, 2656–2676 (2010)
35. S. Oehms, Centralizer coalgebras, FRT-construction, and symplectic monoids. J. Algebra **244**, 19–44 (2001)
36. C.M. Ringel, The category of modules with good filtrations over a quasi-hereditary algebra has almost split sequences. Math. Z. **208**, 209–223 (1991)
37. R. Rouquier, q-Schur algebras and complex reflection groups. Moscow Math. J. **8**, 119–158 (2008)
38. I. Schur, Über die rationalen Darstellungen der allgemeinen linearen Gruppe. Sitzungsberichte Akad. Berlin, 58–75 (1927) (Reprinted as: I. Schur, *Gesammelte Abhandlungen III* (Springer, Berlin, 1973), pp. 68–85)
39. L.L. Scott, Simulating algebraic geometry with algebra I: the algebraic theory of derived categories. Proc. Symp. Pure Math. **47**, 271–281 (1987)
40. R. Tange, The symplectic ideal and a double centraliser theorem. J. Lond. Math. Soc. (2) **77**(3), 687–699 (2008)
41. H. Wenzl, On the structure of Brauer's centralizer algebras. Ann. Math (2) **128**(1), 173–193 (1988)

Arithmetic Functions: A Pivotal Topic in the Scientific Work of Wolfgang Schwarz

Karl-Heinz Indlekofer

Dedicated to the memory of my academic teacher Wolfgang Schwarz

Abstract The purpose of this article is to describe some questions which have arisen from discussions in the working group of Wolfgang Schwarz in the early 1970s. We concentrate on problems concerning arithmetical functions and deal with investigations of almost-even, limit-periodic, and almost-periodic functions. We give a survey of relevant results by Schwarz and Schwarz–Spilker, respectively, and add corresponding contributions of the author.

Keywords Almost-even and almost-periodic functions • Asymptotic results on arithmetical functions • Boundary behavior of power series • Compactifications of $\mathbb{N}$ and integration • Conformally equivalent series • Power series methods of summability • Ramanujan expansions • Uniformly summable functions

2010 Mathematics subject classification: Primary 11K65; Secondary 11N37, 11N56, 11N60, 11N64, 30B30, 40G05, 40G10

1 A Selection of Mathematical Subjects Discussed in the Group of Wolfgang Schwarz in the Early 1970s

When I came to Frankfurt in October 1969 as an assistant in the working group of Wolfgang Schwarz the initial phase was characterized by the involvement with the doctoral dissertation and preoccupation with various mathematical topics treated by Schwarz in his lectures and seminars. I could benefit a lot from his motivating and inspiring suggestions. In this article I will describe the main topics discussed in the

K.-H. Indlekofer (✉)
Faculty of Computer Science, Electrical Engineering and Mathematics, University of Paderborn, Warburger Straße 100, 33098 Paderborn, Germany
e-mail: k-heinz@math.uni-paderborn.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_12

Group of Wolfgang Schwarz in 1970. Published with kind permission of © Karl-Heinz Indlekofer, 1970

group of Wolfgang Schwarz during the early 1970s. I present the related results of Schwarz referring in many cases to the monograph [62] of Schwarz and Spilker. Additionally, I complement this survey by results which I could contribute to these topics.

I. Equivalent power series

In 1958, *equivalent power series* were introduced by Turán [63]. To this end let $D := \{z \in \mathbb{C} : |z| < 1\}$ be the open unit disk and $\bar{D} := \{z \in \mathbb{C} : |z| \leq 1\}$ the closed unit disk of the complex plane, and denote by $H(D)$ the algebra of all holomorphic functions in D. If $\zeta \in D$, $\zeta \neq 0$, then

$$\phi_\zeta(z) = \frac{1-\bar{\zeta}}{1-\zeta} \cdot \frac{z-\zeta}{1-\bar{\zeta}z}$$

defines a conformal and bijective mapping ϕ_ζ of $\overline{D}$ onto itself with $\phi_\zeta(1) = 1$. If $f \in H(D)$, then $f_1 = f \; o \; \phi_\zeta \in H(D)$, and the Taylor series representing f and f_1, respectively, are called *conformally equivalent.*

Turán investigated the periphery-convergence behavior of equivalent power series, and he showed that the convergence is not conformally equivalent. More explicitly this means the following: he proved the existence of functions $f \in H(D)$,

the Taylor series

$$f(w) = \sum_{k=0}^{\infty} a_k w^k \tag{1.1}$$

of which converges for $w = 1$, whereas the power series

$$f_1(z) = f(\phi_\zeta(z)) = \sum_{k=0}^{\infty} b_n(\zeta) z^n \tag{1.2}$$

diverges for $z = \phi_\zeta^{-1}(1) = 1$. Such a function is called *konvergenz-schlecht* (badly convergent) under ϕ_ζ (see Schwarz [51]). In 1967, Clunie [3] gave, for each fixed $0 < |\zeta| < 1$, an example of a function $f \in H(D)$, which is continuous on $\overline{D}$, such that (1.1) converges for $w = 1$ and the transformed series (1.2) diverges for $z = 1$. In the same year Schwarz [51] sharpened Clunie's result by using the theorem of Banach–Steinhaus. In [52] he investigated functions $f \in H(D)$ which satisfy some certain modulus of continuity on the boundary of D and are badly convergent under ϕ_ζ. These results motivated and influenced my dissertation which is published in [13, 14, 16]. In [15] I could improve the result of Schwarz [52] by verifying a conjecture of Paul Turán. A more detailed discussion of this topic may be found in [38] and in the survey article [31].

II. Multiplicative functions of modulus ≤ 1

The results of Delange [9], Wirsing [66], and Halász [12] aroused the interest of Wolfgang Schwarz in the investigation of multiplicative functions. For arithmetical functions $f : \mathbb{N} \to \mathbb{C}$ let us denote *the means of* f by

$$M(f, x) := \frac{1}{x} \sum_{n \leq x} f(n)$$

and call

$$M(f) := \lim_{x \to \infty} M(f, x) \tag{1.3}$$

the *mean-value* of f if the limit (1.3) exists. Delange [9] essentially characterized those multiplicative functions f, $|f| \leq 1$, for which the mean-value $M(f)$ exists and is different from zero. Wirsing [66] showed in 1967 that every *real-valued* multiplicative function of modulus ≤ 1 possesses a mean-value and solved an old conjecture of Erdös and Wintner: *Any multiplicative function f, assuming only the values* $1, 0$, *and* -1, *possesses a mean-value.* Choosing $f = \mu$, the Möbius function, this result implies the prime number theorem.

One year later Halász [12] gave a complete description of the asymptotic behavior of $M(f, x)$, $|f| \leq 1$, and showed:

Let $f : \mathbb{N} \to \mathbb{C}$ be multiplicative of modulus $|f| \le 1$. Then there exist constants c, a_0 and a slowly oscillating function L of modulus $|L| = 1$, so that the asymptotic formula

$$\sum_{n \le x} f(n) = c x^{1+ia_0} L(\log x) + o(x)$$

is true.

Motivated by papers of Novoselov [47, 48] which we discussed in our Seminar (1971/72), the question was posed whether, for functions f occurring in Halász's result and possessing a mean-value $M(f)$, this mean-value can be represented as an integral.

The idea of Novoselov was, briefly summarized, as follows:

- The ring $\mathbb{Z}$ of the integers is embedded into the compact topological ring S of the polyadic numbers.
- Then, on the additive group of the ring S, as a compact group, there exists a normalized Haar measure P defined on a σ-algebra $\mathcal{A}$ which contains the Borel sets in S such that $(S, \mathcal{A}, P)$ is a probability space and P is the extension of the asymptotic density.
- This enabled Novoselov to develop an "integration theory" for the space of *limit-periodic functions*, i.e., for arithmetic functions which can be approximated by periodic functions with integer period.

Then the posed question may be formulated as

Problem: Let f be a multiplicative function such that the mean-value $M(f)$ exists. Is it possible to represent $M(f)$ as an integral

$$M(f) = \int_{\overline{\mathbb{N}}} \bar{f} d\rho$$

where $\overline{\mathbb{N}}$ is a compactification of $\mathbb{N}$, $\bar{f}$ is an extension of f to $\overline{\mathbb{N}}$, and ρ is an appropriate measure on $\overline{\mathbb{N}}$?

III. Spaces of arithmetical functions

This topic is closely connected with the problem of extending the results of Delange, Wirsing, and Halász, respectively, to "unbounded" (multiplicative) functions.

To start from the beginning we denote by $\mathcal{B}$ and $\mathcal{D}$ the spaces of all *even functions* and all *periodic functions*, respectively. The base for further questions was the very nice paper by Schwarz and Spilker [61] in 1971. They showed that $\mathcal{B}$ is equal to the space of all linear combinations of *Ramanujan sums* c_r where

$$c_r(n) = \sum_{\substack{1 \le a \le r \\ gcd(a,r)=1}} e_{a/r}(n)$$

and every $f \in \mathcal{D}$ can be written as a linear combination of the exponential functions $e_{a/r}$,

$$e_{a/r}(n) = \exp(2\pi i \frac{a}{r} n) \ \ (a, r \in \mathbb{N})$$

i.e.,

$$\mathcal{B} = Lin_{\mathbb{C}}[c_r : r = 1, 2, \ldots]$$
$$\mathcal{D} = Lin_{\mathbb{C}}[e_{a/r} : r = 1, 2, \ldots; 1 \le a < r, gcd(a, r) = 1].$$

In addition, define the vector space

$$\mathcal{A} := Lin_{\mathbb{C}}[e_\alpha : \alpha \in \mathbb{R} \ \ mod \ \ \mathbb{Z}]$$

of complex linear combinations of e_α. Taking the closure of $\mathcal{B}, \mathcal{D}$, and $\mathcal{A}$ with respect to the supremum norm $\|.\|_u$, defined by

$$\|f\|_u := \sup_{n \in \mathbb{N}} |f(n)| \ \ for \ f \in \ell^\infty,$$

we arrive at the spaces

$$\mathcal{B}^u : \|.\|_u \ \ closure \ \ of \ \ \mathcal{B}, \ \ uniformly \ \ almost - even \ \ functions,$$
$$\mathcal{D}^u : \|.\|_u \ \ closure \ \ of \ \ \mathcal{D}, \ \ uniformly \ \ limit - periodic \ \ functions,$$
$$\mathcal{A}^u : \|.\|_u \ \ closure \ \ of \ \ \mathcal{A}, \ \ uniformly \ \ almost - periodic \ \ functions.$$

These three spaces are the starting points for further investigations. They are B^*-algebras

$$\mathcal{B}^u \subset \mathcal{D}^u \subset \mathcal{A}^u \subset \ell^\infty \tag{1.4}$$

and Gelfand's theory can be applied. Further, the mean-value $M(f)$, the Fourier-coefficients $M(fe_\alpha)$, and Ramanujan-coefficients $M(fc_r)$ exist for all $f \in \mathcal{A}^u$ and motivate questions concerning Fourier- and Ramanujan-expansions. The characterization of *multiplicative* functions belonging to these spaces is an obvious question.

When J. Knopfmacher held a visiting professorship in Frankfurt for a period during 1973 he lectured on many topics of his "Abstract analytic number theory" and discussed the question to transfer the above described theory to arithmetical semigroups. In Chap. 7 of his book [40] he describes the generalized Fourier theory of even and almost-even functions. Multiplicative functions on arithmetical semigroups and analogues for Halász's theorem, etc., and similar questions are handled, for example, by Indlekofer and Manstavicius [35, 36] by Barát et al. [2] and by Indlekofer and Kaya [34], but here we will not deal with these topics.

The interest of Wolfgang Schwarz focussed further in the completion of $\mathcal{B}, \mathcal{D}$, and $\mathcal{A}$ with respect to the semi-norm

$$\|f\|_q := \left(\limsup_{x\to\infty} \frac{1}{x}\sum_{n\le x} |f(n)|^q\right)^{1/q}, \quad q \ge 1$$

which he denoted by

$$\mathcal{B}^q, \quad \mathcal{D}^q, \quad \text{and} \quad \mathcal{A}^q, \quad \text{respectively,}$$

the spaces of *q-almost-even, q-almost-limit-periodic, and q-almost-periodic* functions. Here again the mean-values $M(f), M(fe_\alpha)$, and $M(fc_r)$ exist for every $f \in \mathcal{A}^q$. In this context he dealt with questions about

(i) (general) properties of q-almost-periodic functions,
(ii) characterizations and properties of multiplicative functions from $\mathcal{B}^q$, $\mathcal{D}^q$, and $\mathcal{A}^q$,
(iii) pointwise convergence of Ramanujan expansions for multiplicative functions.

In this paper we describe the results obtained for (ii) and (iii) which can be found in the monograph [62] by Schwarz and Spilker and add some aspects which are not included in the book (cf. Preface of [62], p. xiii). For example, we deal with the $\|.\|_1$-closure of ℓ^∞, the space $\mathcal{L}^*$ of *uniformly summable* functions (cf. [62]) and give the characterization of the multiplicative functions $f \in \mathcal{L}^*$ (independent whether the mean-value $M(f)$ exists or not). We describe the answer of Schwarz and Spilker to the problem of representing the mean-value as an integral and compare it with a method introduced by me in 1992 (see [25], Preface of [62], p. xiii, and [60], Sect. 6.3).

2 Characterization of Multiplicative Functions in $\mathcal{B}^q \subset \mathcal{D}^q \subset \mathcal{A}^q \subset \mathcal{L}^*$

2.1 Multiplicative Functions in $\mathcal{L}^*$ with Non-zero Mean-Value

For $q \ge 1$ let

$$\mathcal{L}^q = \{f : \mathbb{N} \to \mathbb{C}, \|f\|_q < \infty\}$$

be the vector space of functions f with bounded semi-norm $\|f\|_q$. Obviously

$$\mathcal{B}^q \subset \mathcal{D}^q \subset \mathcal{A}^q \subset \mathcal{L}^q \subset \mathcal{L}^* \subset \mathcal{L}^1 \quad \text{if} \quad q > 1.$$

In 1980, I [17] could prove

Theorem 2.1 *Let $f : \mathbb{N} \to \mathbb{C}$ be multiplicative and $q \geq 1$. Then the following two assertions hold:*

(i) *If $f \in \mathcal{L}^* \cap \mathcal{L}^q$ and if the mean-value $M(f)$ exists and is different from zero, then the series*

$$\sum_p \frac{f(p)-1}{p} \ , \ \sum_{|f(p)|\leq \frac{3}{2}} \frac{|f(p)-1|^2}{p} \tag{2.1}$$

and

$$\sum_{\substack{p \\ |f(p)-1|\geq \frac{1}{2}}} \frac{|f(p)|^\lambda}{p} \ , \ \sum_p \sum_{k\geq 2} \frac{|f(p^k)|^\lambda}{p^k} \tag{2.2}$$

converge for all λ with $1 \leq |\lambda| \leq q$ and, for each prime p,

$$1 + \sum_{k=1}^{\infty} \frac{f(p^k)}{p^k} \neq 0. \tag{2.3}$$

(ii) *If the series (2.1) and (2.2) converge, then $f \in \mathcal{L}^* \cap \mathcal{L}^q$, and the mean-values $M(f), M(|f|^\lambda)$ exist for all λ with $1 \leq \lambda \leq q$. If in addition (2.3) holds, then $M(f) \neq 0$.*

Elliott proved the assertions of Theorem 2.1 for $q = 2$ in 1975 [10] and for $q > 1$ in 1980 [11]. Daboussi [5] published a proof for the case $q > 1$ in 1981. A general characterization of uniformly summable multiplicative functions will be described in Sect. 2.4.

2.2 Multiplicative Functions in $\mathcal{B}^q$, $\mathcal{D}^q$, and $\mathcal{A}^q$ with Non-zero Mean-Value

It turns out that these functions are just the same as those in 2.1. From [62] we cite

Theorem 2.2 ([62], Chap. VII, Theorem 5.1) *Let f be a multiplicative arithmetical function with mean-value $M(f) \neq 0$. Assume that $q \geq 1$. Then the following statements are equivalent:*

(1) The series (2.1) and (2.2) converge for $\lambda = q$.
(2) $f \in \mathcal{B}^q$,
(3) $f \in \mathcal{D}^q$,
(4) $f \in \mathcal{A}^q$.

If $q \geq 2$, then (1) *to* (4) *are equivalent to*

(5) $\|f\|_q < \infty$.

Furthermore, in any case and for every prime p,

$$1 + p^{-1}f(p) + p^{-2}f(p^2) + \ldots \neq 0.$$

Obviously each of conditions (1)–(4) is equivalent to $f \in \mathcal{L}^q \cap \mathcal{L}^*$, and is equivalent to $\|f\|_q < \infty$, if $q > 1$.

2.3 Multiplicative Functions in $\mathcal{B}^q$, $\mathcal{D}^q$, and $\mathcal{A}^q$ with Mean-Value Zero

If the mean-value equals zero the situation differs considerably from the previous one and leads to results distinguishing between q-almost-even and q-limit-periodic functions. For this we define the *Fourier-Bohr spectrum* $\sigma(f)$ of f by

$$\sigma(f) := \{\alpha \in \mathbb{R}/\mathbb{Z} : \limsup_{x\to\infty} x^{-1} |\sum_{n\leq x} f(n) \exp(-2\pi i n\alpha)| > 0\}.$$

The *Ramanujan spectrum* $\sigma^*(f)$ of f is the set

$$\sigma^*(f) := \{r \in \mathbb{N} : \limsup_{x\to\infty} x^{-1} |\sum_{n\leq x} f(n)c_r(n)| > 0\}.$$

In 1981, I [19] proved the following results:

Theorem 2.3 *Let $f : \mathbb{N} \to \mathbb{C}$ be multiplicative and $q \geq 1$. Then the following assertions are equivalent:*

(i) $f \in \mathcal{B}^q$ *and* $\|f\|_1 > 0$.
(ii) $f \in \mathcal{B}^q$ *and the spectrum* $\sigma^*(f)$ *of* f *is non-empty.*
(iii) $f \in \mathcal{L}^q \cap \mathcal{L}^*$ *and there exists a principal Dirichlet-character* χ_0 *so that the mean-value* $M(f\chi_0)$ *of* $f\chi_0$ *exists and is different from zero.*
(iv) The series (2.1) and (2.2) converge for all λ *with* $1 \leq \lambda \leq q$.

The case $|f| \leq 1$ was handled by Schwarz and Spilker in [62], Theorem 5.1. The main content of Theorem 2.3 may be found in the Exercises 2 and 3 of VII.7 in [62].

Theorem 2.4 *Let $f : \mathbb{N} \to \mathbb{C}$ be multiplicative and $q \geq 1$. Then the following assertions are equivalent:*

(i) $f \in \mathcal{D}^q$ *and* $\|f\|_1 > 0$.
(ii) $f \in \mathcal{D}^q$ *and the spectrum* $\sigma(f)$ *of* f *is non-empty.*

(iii) $f \in \mathcal{L}^q \cap \mathcal{L}^*$ *and there exists a Dirichlet-character* χ *so that the mean-value* $M(f\chi)$ *of* $f\chi$ *exists and is different from zero.*

(iv) There exists a Dirichlet-character χ *such that the series*

$$\sum_p \frac{f(p)\chi(p)-1}{p}, \quad \sum_{\substack{p \\ |f(p)|\le\frac{3}{2}}} \frac{|f(p)\chi(p)-1|^2}{p} \tag{2.4}$$

and (2.2) converge for all λ *with* $1 \le \lambda \le q$.

The equivalence of (ii) and (iv) was proved by Daboussi [4]. Schwarz and Spilker deal with this equivalence in Theorem 6.1 of Chap. VII in [62].

In the proof of Theorem 2.4, I used the fact that if $f \in \mathcal{L}^*$ is multiplicative then $\sigma(f)$ contains only rational values. This result is best possible in the sense that there are multiplicative functions $f \in \mathcal{L}^1 \backslash \mathcal{L}^*$ such that $\sigma(f)$ contains irrational values. Further, the result says that if $f \in \mathcal{A}^q$ is multiplicative, then $f \in \mathcal{D}^q$. Daboussi (see [6] and [46]) gave a proof of this result for bounded multiplicative functions, where Daboussi–Delange's paper [7] treats the case $f \in \mathcal{L}^2$. In Lemma 6.3 of Chap. VII in [62] Schwarz and Spilker give a proof for $f \in \mathcal{A}^1$.

Further generalizations may be found in the papers [32] and [33] by Indlekofer and Kátai.

2.4 Multiplicative Functions in $\mathcal{L}^*$

Using the same proof as in [17] one can prove the following characterization:

Theorem 2.5 *Let* $f \in \mathcal{L}^*$ *be multiplicative and* $\|f\|_1 > 0$. *Then the series*

$$\sum_{\substack{p \\ ||f(p)|-1|>\frac{1}{2}}} \frac{1}{p}, \quad \sum_{\substack{p \\ ||f(p)|-1|>\frac{1}{2}}} \frac{|f(p)|}{p} \tag{2.5}$$

and (2.2) converge for $\lambda = 1$, *and there exists a sequence* $1 \le x_1 < x_2 < \ldots \nearrow \infty$ *such that the partial sums*

$$\sum_{p \le x_k} \frac{|f(p)|-1}{p} \tag{2.6}$$

are uniformly bounded $(k = 1, 2, \ldots)$.

This implies, with the method given in [17],

Theorem 2.6 *Let $f \in \mathcal{L}^*$ be multiplicative and $\|f\|_1 > 0$. Then there exists a constant $c > 0$ such that*

$$x^{-1} \sum_{n \le x} |f(n)| = \exp\left(\sum_{p \le x} \frac{|f(p)| - 1}{p} \right) (c + o(1)) \tag{2.7}$$

as $x \to \infty$.

Since the sequence $\{M(|f|, n)\}$ of the means is bounded, (2.7) implies that there exists a constant c' such that

$$\sum_{p \le x} \frac{|f(p)| - 1}{p} \le c' \quad \text{for all } x \ge 2. \tag{2.8}$$

Repeating the arguments used in [17], Sect. 4, word by word, one can show that (2.8) and the necessary conditions in Theorem 2.5 imply that $f \in \mathcal{L}^*$ and $\|f\|_1 > 0$. Further, one concludes that $\|f\|_1 = 0$ if and only if one of the series in (2.2) or (2.5) diverges or the sum in (2.6) tends to ∞ for all sequences $\{x_k\}, x_k \to \infty$.

A general representation for multiplicative functions in $\mathcal{L}^*$ is given in

Theorem 2.7 *Let $f \in \mathcal{L}^*$ be multiplicative and $\|f\|_1 > 0$. Then either the mean-value $M(f)$ exists and equals zero or there exist constants $a_0 \in \mathbb{R}$ and $0 \ne c_0 \in \mathbb{C}$ such that, as $x \to \infty$,*

$$x^{-1} \sum_{n \le x} f(n) = x^{ia_0} \exp\left(\sum_{p \le x} \frac{f(p)p^{-ia_0} - 1}{p} \right) \cdot (c_0 + o(1)).$$

If

$$A^*(x) := \sum_{p \le x} \frac{Imf(p)p^{-ia_0}}{p}$$

then

$$\lim_{x \to \infty} \sup_{x \le y \le x^2} |A^*(y) - A^*(x)| = 0$$

If the mean-value $M(|f|)$ exists, then the proof of Theorem 2.7 can be found in [18]. For the general case, see [22].

As a consequence of Theorem 2.7 we mention a generalization of the cited result by Wirsing.

Corollary 2.8 *Let $f \in \mathcal{L}^*$ be real-valued and multiplicative. If $M(|f|)$ exists, then $M(f)$ exists.*

Concluding remarks For a quantitative form of Wirsing's result we refer to [30]. The connections of the above results with the existence of the limiting distribution of multiplicative functions and the characterization of additive functions are described in [20, 21, 24] and in [23], respectively. In the final chapter of [62] Schwarz and Spilker present the *elementary proofs* of the cited Halász's theorem by Daboussi and Indlekofer [8]. For supplementary informations see [26] and [29].

2.5 *Pointwise Convergence of Ramanujan Expansions for Multiplicative Functions in* $\mathcal{B}^1$

With their paper [61] Schwarz and Spilker start up a Fourier theory for almost-even functions. For example, the set $\{(\varphi(r))^{-\frac{1}{2}}c_r : r = 1, 2, \ldots\}$ is a complete orthonormal system in $\mathcal{B}^2$ and Parseval's equation holds. Every $f \in \mathcal{B}^1$ possesses a Ramanujan expansion

$$f = \sum_r a_r(f)c_r$$

where the (Ramanujan) coefficients $a_r(f)$ are given by

$$a_r(f) = \frac{1}{\varphi(r)}M(fc_r).$$

Therefore it becomes of interest to investigate the pointwise convergence to f of the associated Ramanujan series. From 1973 to 1975 Schwarz dedicated himself to this problem in the case of multiplicative functions (see [53–59]) and succeeded to verify the following:

Theorem 2.9 *Let f be multiplicative of modulus $|f| \leq 1$. If $M(f) \neq 0$, then its associated Ramanujan expansion is pointwise convergent and*

$$\sum_{r=1}^{\infty} a_r(f)c_r(n) = f(n) \text{ for any } n \in \mathbb{N}. \tag{2.9}$$

In 1980, Tuttas [64] extended this result to multiplicative functions with non-zero mean-value belonging to $\mathcal{B}^2$. In 1983, using [17], Warlimont [65] showed that if $f \in \mathcal{B}^1$ is multiplicative and if the series (2.1) and (2.2) converge, then (2.9) holds. Bearing in mind Theorem 2.1 and by Warlimont's result we get immediately the following refinement of Theorem 2.9:

Theorem 2.10 *Let $f \in \mathcal{B}^1$ be multiplicative and $\|f\|_1 > 0$. Then the assertion of Theorem 2.9 holds true.*

There are some fascinating examples of pointwise convergent Ramanujan expansions for particular functions of interest, which cannot be explained in the previous context. For example, the following formulas for the divisor function $d(n)$ and the counting function $r(n)$ of the numbers of representations of n in the form $n = a^2+b^2$ $(a, b \in \mathbb{Z})$ have been established by Ramanujan [50]:

$$d(n) = -\sum_{k=1}^{\infty} \frac{\log k}{k} c_k(n) \tag{2.10}$$

$$r(n) = \pi \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{2k-1} c_{2k-1}(n) \tag{2.11}$$

The fact that the formulae do not fit within the previous framework is obvious in the first case since the mean-value of d does not exist. In the second case, the function r has the form $r = 4(1 * \chi)$ with the non-principal Dirichlet-character χ *mod* 4. The mean-value $M(r)$ exists and equals π, so that (2.11) has the general appearance as the formula considered in Theorem 2.9. Further, it shows that $r \in \mathcal{L}^1$ but it turns out by Theorem 2.1 that r is *not* uniformly summable.

A concept which can handle such "mysterious" Ramanujan expansions and which is not based on almost-even functions has been introduced by Lucht [43] in 1993. In his article [44] he gives a detailed description of this topic.

3 Integration

3.1 Integration via Gelfand Representation

The algebra $\mathcal{B}^u$ is a commutative algebra with identity which is closed under the involution $f \to \bar{f}$ (complex conjugation). Therefore the Gelfand Representation Theorem is applicable and implies that $\mathcal{B}^u$ is isomorphic and isometric to the algebra $C(X)$ of all continuous complex-valued functions on a certain compact Hausdorff space X—its maximal ideal space, denoted by $X = \Delta_{\mathcal{B}}$. The following theorem, which does not depend on the Gelfand Representation Theorem, provides slightly sharper information as to how (uniformly) almost-even functions can be represented by continuous functions on an explicit compact space. For this Schwarz and Spilker [61] introduced the compactification $\mathbb{N}^*$ of $\mathbb{N}$ by

$$\mathbb{N}^* = \prod_{\substack{p \\ prime}} N_p$$

where N_p the one-point compactification of the discrete (and locally compact) space $(1, p, p^2, \ldots)$.

Theorem 3.1 *Let*

$$\iota : \mathbb{N} \to \mathbb{N}^*$$

be the embedding of $\mathbb{N}$ *into* $\mathbb{N}^*$. *Then the induced homomorphism*

$$\iota^* : C(\mathbb{N}^*) \to \ell^\infty, \quad \iota^* F = F \circ \iota$$

maps $C(\mathbb{N}^*)$ *isomorphically and isometrically onto* $\mathcal{B}^u$.

Knopfmacher [40] transferred this theorem to arithmetical semigroups. In [62], Chap. IV, Schwarz and Spilker describe the Gelfand's theory for the algebras $\mathcal{B}^u$ and $\mathcal{D}^u$.

In the case $\mathcal{D}^u$ of (uniformly) limit-periodic functions they show that the maximal ideal space $\Delta_{\mathcal{D}}$ of $\mathcal{D}^u$ is homeomorphic to the Prüfer Ring $\hat{\mathbb{Z}}$. In order to define $\hat{\mathbb{Z}}$, first consider any n and the residue class ring $\mathbb{Z}/n\mathbb{Z}$ with the discrete topology. Now form the topological product $X = \prod_n \mathbb{Z}/n\mathbb{Z}$. Finally, consider the natural projection

$$\pi_{m,n} : \mathbb{Z}/\mathbb{Z}_n \to \mathbb{Z}/\mathbb{Z}_m, \quad \textit{if} \quad m|n$$

and define the compact space $\hat{\mathbb{Z}}$ by the projective limit

$$\hat{\mathbb{Z}} := \{(\alpha_n) \in X : \alpha_n \in \mathbb{Z}/\mathbb{Z}_n \ \textit{and} \ \pi_{m,n}(\alpha_n) = \alpha_m, \ \textit{if} \ m|n\}.$$

Mauclaire [45] showed that the Bohr compactification of $\mathbb{Z}$ is the appropriate space for corresponding investigations of (uniformly) almost-periodic functions.

Remark The compactification $\hat{\mathbb{Z}}$ was given by Prüfer [49] in 1925. In 2002, Kubota and Sugita [42] introduced a compactification $\tilde{\mathbb{Z}}$ of $\mathbb{Z}$ by $\tilde{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ where $\mathbb{Z}_p$ denotes the ring of p-adic integers. It turns out (see Barát et al. [1]) that the compact rings of Prüfer, Novoselov, and Kubota–Sugita are homeomorphic to each other.

The construction of Schwarz and Spilker for an "integration theory on $\mathcal{B}^u$" is now straightforward.

The mean-value $M(f)$ of f is a nonnegative linear functional on $\mathcal{B}^u$. It is bounded (and continuous) and extends uniquely to $C(\mathbb{N}^*)$ by

$$M^* : C(\mathbb{N}^*) \to \mathbb{C}$$
$$M^*(F) = M(f \circ \iota) \ \textit{for every} \ F \in C(\mathbb{N}^*).$$

Then M^* is a bounded, nonnegative linear functional and Riesz's Theorem yields

Theorem 3.2 (see [62], Chap. IV, Theorem 6.1) *There exists a complete and regular probability measure* δ, *defined on a* σ- *algebra* $\mathcal{A}$, *containing the Borel*

sets of $\mathbb{N}^*$*, with the property*

$$\int_{\mathbb{N}^*} F d\bar{\delta} = M^*(F) = M(Fo\,\iota)$$

for every $F \in C(\mathbb{N}^*)$.

The measure $\bar{\delta}$ and the σ -algebra $\mathcal{A}$ can be characterized as a product measure on $\mathbb{N}^* = \prod_p N_p$ and via the product σ-algebra of $\mathbb{N}^*$, respectively. For details, see [62], Chap. IV.

In 1976, Knopfmacher [41] showed that the quotient space $\mathcal{B}^q/$ nullspace corresponds to $L^q(\mathbb{N}^*, \bar{\delta})$, and that the whole theory can be extended to arithmetical semigroups.

Similar conclusions as in Theorems 3.1 and 3.2 can be done for the B^*-algebras $\mathcal{D}^u$ and $\mathcal{A}^u$. But Schwarz and Spilker did not follow up this topic. It should be alluded the special role played by the asymptotic density in the investigations of the spaces $\mathcal{B}^u, \mathcal{D}^u$, and $\mathcal{A}^u$. Further, despite of the *ad hoc* construction of the compactifications, the "size" of these spaces is "restricted"; the Möbius μ function, for example, is not an element of any of these spaces. To avoid these limitations the author described in the 1990s an "integration theory" which is based on the Stone–Čech compactification of the natural numbers.

3.2 Integration via the Stone–Čech Compactification

Suppose that $\mathcal{A}$ is an algebra of subsets of $\mathbb{N}$, i.e.,

(i) $\mathbb{N} \in \mathcal{A}$
(ii) $A, B \in \mathcal{A} \Rightarrow A \cup B \in \mathcal{A}$
(iii) $A, B \in \mathcal{A} \Rightarrow A \setminus B \in \mathcal{A}$

Then, if $\mathcal{E}$ denotes the family of simple functions on $\mathbb{N}$, the set

$$\mathcal{E}(\mathcal{A}) := \{s \in \mathcal{E}, s = \sum_{j=1}^{m} \alpha_j 1_{A_j};\ \alpha_j \in \mathbb{C},\ A_j \in \mathcal{A},\ j = 1, \dots, m\}$$

of simple functions on $\mathcal{A}$ is a vector space, especially an algebra, such that $\mathcal{E}(\mathcal{A})^u$, the $\|.\|_u$ -closure of $\mathcal{E}(\mathcal{A})$, is a B^*-algebra.

The main difficulties concerning the immediate application of probabilistic tools to the investigation of additive and multiplicative functions in number theory arise from the fact that the asymptotic density defines only a finitely additive measure on the family of subsets of $\mathbb{N}$ having an asymptotic density. To overcome these difficulties we proceed as follows: $\mathbb{N}$, endowed with the discrete topology, will be embedded in a compact space $\beta\mathbb{N}$, the Stone–Čech compactification of $\mathbb{N}$, and then

any algebra $\mathcal{A}$ in $\mathbb{N}$ with an arbitrary finitely additive set function, a content or pseudomeasure on $\mathbb{N}$, can be extended to an algebra $\bar{\mathcal{A}}$ in $\beta\mathbb{N}$ together with an extension of this pseudomeasure, which turns out to be a premeasure on $\bar{\mathcal{A}}$. The basic necessary concepts are summarized in the following three propositions:

Proposition 3.3 *There exists a compactification $\beta\mathbb{N}$ of $\mathbb{N}$ with the following equivalent properties:*

(i) *Every mapping f from $\mathbb{N}$ into any compact space Y has a continuous extension $\bar{f}$ from $\beta\mathbb{N}$ into Y.*
(ii) *Every function from ℓ^∞ has an extension to a function in $C(\beta\mathbb{N})$.*
(iii) *For any two subsets A and B of $\mathbb{N}$,*

$$\overline{A \cap B} = \bar{A} \cap \bar{B}$$

where $\bar{A} = cl_{\beta\mathbb{N}}A$ and $\bar{B} = cl_{\beta\mathbb{N}}B$ are the closures of A and B in $\beta\mathbb{N}$, respectively.
(iv) *Any two disjoint subsets of $\mathbb{N}$ have disjoint closures in $\beta\mathbb{N}$.*

An immediate consequence of (iii) is the following statement:

Proposition 3.4 *The compactification $\beta\mathbb{N}$ of $\mathbb{N}$ has the following property:*

(v) *For any algebra $\mathcal{A}$ in $\mathbb{N}$, the family*

$$\bar{\mathcal{A}} := \{\bar{A} : A \in \mathcal{A}\}$$

is an algebra in $\beta\mathbb{N}$.

This property is equivalent to properties (i)–(iv) of Proposition 3.3.

It should be observed that $\beta\mathbb{N}$ is unique in the following sense: if a compactification $\tilde{\mathbb{N}}$ of $\mathbb{N}$ satisfies any one of the listed conditions, then there exists a homeomorphism of $\beta\mathbb{N}$ onto $\tilde{\mathbb{N}}$ that leaves $\mathbb{N}$ pointwise fixed.

As a consequence of Property (i), we obtain the following:

The identity mapping $\imath : \mathbb{N} \to \mathbb{N}$ is a continuous monomorphism, which sends $\mathbb{N}$ onto a dense subset of $\beta\mathbb{N}$, such that the adjoint homomorphism

$$\imath^* : C(\beta\mathbb{N}) \to \ell^\infty, \quad \imath^*(\bar{f}) = \bar{f} o\, \imath,$$

maps $C(\beta\mathbb{N})$ isomorphically and isometrically onto ℓ^∞.

We are now in position to formulate the following fundamental result:

Proposition 3.5 *Let $\mathcal{A}$ be an algebra in $\mathbb{N}$ and $\delta : \mathcal{A} \to [0, \infty)$ be a content on $\mathcal{A}$. Then, the map*

$$\bar{\delta} : \bar{\mathcal{A}} \to [0, \infty), \quad \bar{\delta}(\bar{A}) = \delta(A),$$

is σ-additive on $\bar{\mathcal{A}}$ and can uniquely be extended to a measure on the minimal σ-algebra $\sigma(\bar{\mathcal{A}})$ over $\bar{\mathcal{A}}$.

We remark, as an immediate implication of the above construction, the following:

(i) Every finitely additive function on an algebra $\mathcal{A}$ in $\mathbb{N}$ can be extended to a finitely additive function on the algebra of all subsets of $\mathbb{N}$.
(ii) Every linear functional on the vector space $\mathcal{E}(\mathcal{A})$ can be extended to a linear functional on ℓ^∞.

Let us now assume that every $A \in \mathcal{A}$ possesses an asymptotic density $\delta(\mathcal{A})$ and define:

For a given algebra $\mathcal{A}$ and for $q \geq 1$ denote by $\mathcal{L}^{*q}(\mathcal{A})$ the $\|.\|_q$ closure of $\mathcal{E}(\mathcal{A})$. A function $f \in \mathcal{L}^{*q}(\mathcal{A})$ is called *q-uniformly $(\mathcal{A})$-summable.* By $L^{*q}(\mathcal{A})$ we denote the quotient space $\mathcal{L}^{*q}(\mathcal{A})$ modulo null functions.

A first consequence of the above construction is that, for all $s \in \mathcal{E}(\mathcal{A})$,

$$M(s) = \int\limits_{\beta\mathbb{N}} \bar{s} d\bar{\delta}$$

where $\bar{s} : \beta\mathbb{N} \to \mathbb{C}$ denotes the extension of s.

Starting from this one arrives at integrable function on the probability space $(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta})$ and

$$L^1(\bar{\delta}) := L^1((\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta})) := \{\bar{f} : \beta\mathbb{N} \to \mathbb{C}, \|\bar{f}\| < \infty\}$$

where

$$\|\bar{f}\| := \int\limits_{\beta\mathbb{N}} |\bar{f}| d\bar{\delta}.$$

There exists a vector-space isomorphism between the spaces $L^*(\mathcal{A})$ and $L^1(\bar{\delta})$ (for details cf. [27–29]). The same conclusions hold for $L^{*q}(\mathcal{A})$ and $L^q(\bar{\delta})$ if $q > 1$.

We shall apply the outlined construction to three examples and establish the relations to the results of Schwarz and Spilker. Further, we show how our construction of integration is related to Gelfand's theorem. Finally, we determine a complete orthonormal system for a Hilbert space whose elements can be approximated by linear combinations of multiplicative functions.

Example 1 Let $\mathcal{A}_1$ be the algebra generated by all zero residue classes. The asymptotic density is a content on $\mathcal{A}_1$,

$$\mathcal{E}(\mathcal{A}_1)^u = \mathcal{B}^u,$$

and

$$L^{*q}(\mathcal{A}_1) = \mathcal{B}^q/nullspace, \quad q \geq 1.$$

Example 2 The algebra $\mathcal{A}_2$, generated by all residue classes, is our second example. Here again the asymptotic density is a finitely additive function on $\mathcal{A}_2$ and

$$\mathcal{E}(\mathcal{A}_2)^u = \mathcal{D}^u.$$

For $q \geq 1$, $L^{*q}(\mathcal{A}_2)$) is isomorphic to the L^q-space of Novoselov's integration theory.

Example 3 Let f be a multiplicative function which assumes only the values $-1, 0$ and 1, and define the sets

$$A_f^+ := \{n : f(n) = 1\}$$
$$A_f^0 := \{n : f(n) = 0\}$$

and

$$A_f^- := \{n : f(n) = -1\}$$

with characteristic functions f^+, f^0, and f^-, respectively. Obviously

$$f^+ = \frac{1}{2}(|f| + f)$$
$$f^0 = 1 - f^+ - f^-$$
$$f^- = \frac{1}{2}(|f| - f).$$

We define the algebra $\mathcal{A}_3$ to be the algebra generated by the sets A_f^+, A_f^0, A_f^- for all multiplicative f with $f(\mathbb{N}) \subset \{-1, 0, 1\}$. An arbitrary set A of $\mathcal{A}_3$ has a characteristic function which is a linear combination of such multiplicative functions, and thus, by Wirsing's theorem, the asymptotic density $\delta(A)$ exists. This leads to the spaces $L^{*q}(\mathcal{A}_3)$ the elements of which can be approximated by linear combinations of multiplicative functions.

The aforementioned connection with Gelfand's theory is described in the following theorem and yields a generalization of Theorem 3.2.

Theorem 3.6 (see Indlekofer and Wagner [37]) *Let $\mathcal{F}$ be a B^*-algebra of complex-valued functions from ℓ^∞ and let L be a positive linear functional on $\mathcal{F}$*

with $L(1_{\mathbb{N}}) = 1$. Then there exists an algebra $\mathcal{A}$ of subsets of $\mathbb{N}$ and a content δ on $\mathcal{A}$ such that

(i) each $f \in \mathcal{F}$ belongs to the $\|.\|_u$-closure of $\mathcal{E}(\mathcal{A})$ and
(ii) for each $f \in \mathcal{F}$ the relation

$$L(f) = \int_{\beta\mathbb{N}} \bar{f} d\bar{\delta}$$

holds.

3.3 Complete Orthonormal Systems

Starting with $\mathcal{B}^u$, $\mathcal{D}^u$, and $\mathcal{A}^u$ an application of Theorem 3.6 leads in any case to some algebra the elements of which possess an asymptotic density.

Let $\mathcal{A}$ be such an algebra. Then, one can define an inner product on $L^{*2}(\mathcal{A})$

$$< f, g >:= M(f\bar{g}), \ \ f, g \in L^{*2}(\mathcal{A}),$$

and by this $L^{*2}(\mathcal{A})$ is a Hilbert space. In [62] Schwarz and Spilker described complete orthonormal systems for their respective spaces and proved

Theorem 3.7 (see Corollary 3.2 in [62], Chap. IV)

(i) The set $\{(\varphi(r))^{-1/2} \cdot c_r, \quad r = 1, 2, \ldots\}$ is a complete orthonormal system in $\mathcal{B}^2$,
(ii) The set $\{e_{a/r}, \quad r = 1, 2, \ldots, \quad 1 \le a \le r, \quad gcd(a, r) = 1\}$ is a complete orthonormal system in $\mathcal{D}^2$,
(iii) The set $\{e_\alpha : \alpha \in \mathbb{R} \ \ mod \ \mathbb{Z}\}$ is a complete orthonormal system in $\mathcal{A}^2$.

Here I sketch the idea how to determine a complete orthonormal system for the Hilbert space $L^{*2}(\mathcal{A}_3)$. For this let

$$\mathcal{R} := \{f : \mathbb{N} \to \mathbb{R}; \ \ f \ \ multiplicative \ \ and \ \ f(\mathbb{N}) \subset \{-1, 1\}\}$$

be the set of all multiplicative functions assuming the values ± 1, and define a relation $\sim$ on $\mathcal{R}$ by

$$f \sim g \ \ \text{iff} \sum_{\substack{p \\ f(p) \neq g(p)}} \frac{1}{p} < \infty.$$

Obviously $\sim$ is an equivalence relation. Now choose a representative from each equivalence class and define $\mathcal{F}_1$ as the complete set of all representatives. If $f, g \in$

$\mathcal{F}_1, f \neq g$, i.e., f and g are not in the same class, then $f(p)g(p)$ takes only the values ± 1, and

$$\sum_p \frac{1 - f(p)g(p)}{p} = \infty.$$

By Wirsing's theorem $M(fg) = 0$. Further, if $f \in \mathcal{F}_1$, then $f^2 = 1$ and $M(f^2) = 1$. This shows that $\mathcal{F}_1$ is an orthonormal system (but not complete). Choosing the normalized Ramanujan functions $c_r^* = (\varphi(r))^{-1/2} c_r$ we put

$$\mathcal{F}_2 := \{f \cdot c_r^* : f \in \mathcal{F}_1, \quad r = 1, 2, \ldots\}$$

which turns out to be a complete orthonormal system for $L^{*2}(\mathcal{A}_3)$. More details can be found in [39].

References

1. A. Barát, K.-H. Indlekofer, R. Wagner, On some compactifications of $\mathbb{N}$, *Analytic and Probabilistic Methods in Number Theory, Proceedings of the 4th International Conference in honour of J. Kubilius held in Palanga*, September 25–29, 2006, Vilnius (2007)
2. A. Barát, K.-H. Indlekofer, E. Kaya, Two series theorem in additive arithmetical semigroups. Ann. Univ. Sci. Budapest. Sect. Comp. **38**, 323–332 (2012)
3. J. Clunie, On equivalent power series. Acta Math. Acad. Sci. Hung. **18**, 165–169 (1976)
4. H. Daboussi, Characterisation des fonctions multiplicatives p.p. B^λ, á spectre non vide. Ann. Inst. Fourier Grenoble **30**, 141–166 (1980)
5. H. Daboussi, Sur les fonctions multiplicatives ayant une valeur moyenne non nulle. Bull. Soc. Math. France **109**, 183–205 (1981)
6. H. Daboussi, H. Delange, Quelques propriétés des fonctions multiplicatives de module au plus égal à 1. C. R. Acad. Sci. Paris Sér. A **278**, 657–660 (1974)
7. H. Daboussi, H. Delange, On multiplicative arithmetical functions whose modulus does not exceed one. J. Lond. Math. Soc. (2) **26**, 245–264 (1982)
8. H. Daboussi, K.-H. Indlekofer, Two elementary proofs of Halász's theorem. Math. Z. **209**, 43–52 (1992)
9. H. Delange, Sur les fonctions arithmétiques multiplicatives. Ann. Sci. Éc. Norm. Super. (3) **78**, 273–304 (1961)
10. P.D.T.A. Elliott, A mean-value theorem for multiplicative functions. Proc. Lond. Math. Soc. **31**, 418–438 (1975)
11. P.D.T.A. Elliott, Mean-value theorems for functions bounded in mean α-power, $\alpha > 1$. J. Austr. Math. Soc. **29**, 177–205 (1980)
12. G. Halász, Über die Mittelwerte multiplikativer Funktionen. Acta Math. Acad. Sci. Hung. **19**, 365–403 (1968)
13. K.-H. Indlekofer, Summierbarkeitsverhalten äquivalenter Potenzreihen I. Arch. Math. **22**, 385–393 (1971)
14. K.-H. Indlekofer, Summierbarkeitsverhalten äquivalenter Potenzreihen II. Math. Nachrichten **50**, 305–319 (1971)
15. K.-H. Indlekofer, Bemerkungen über äquivalente Potenzreihen mit einem gewissen Stetigkeitsmodul. Monatshefte für Mathematik **76**, 124–129 (1972)

16. K.-H. Indlekofer, Summierbarkeitsverhalten äquivalenter Potenzreihen III. Math. Nachrichten **55**, 265–286 (1973)
17. K.-H. Indlekofer, A mean-value theorem for multiplicative arithmetical functions. Math. Zeitschrift **172**, 255–271 (1980)
18. K.-H. Indlekofer, Remark on a theorem of G. Halász. Arch. Math. **36**, 145–151 (1980)
19. K.-H. Indlekofer, Some remarks on almost-even and almost-periodic functions. Arch. Math. **37**, 353–358 (1981)
20. K.-H. Indlekofer, Limiting distributions and mean-values of multiplicative arithmetical functions, in *Recent Progress in Analytic Number Theory, Symposium Durham 1979*, vol. I (Academic, London, 1981), pp. 197–202
21. K.-H. Indlekofer, Limiting distributions and mean-values of multiplicative arithmetical functions. J. für Reine Angew. Math. **328**, 116–127 (1981)
22. K.-H. Indlekofer, Properties of uniformly summable multiplicative functions. Periodica Math. Hung. **17**, 143–161 (1986)
23. K.-H. Indlekofer, Cesáro means of additive functions. Analysis **6**, 1–24 (1986)
24. K.-H. Indlekofer, Limiting distributions and mean-values of complex-valued multiplicative functions, in *Probability Theory and Mathematical Statistics, Proceedings of the 4th Vilnius Conference 1985*, vol. I (1986), pp. 547–552
25. K.-H. Indlekofer, A new method in probabilistic number theory, in *Probability theory and applications: Essays to the memory of József Mogyoródi*, ed. by J. Galambos, I. Kátai (Kluwer, Dordrecht, 1992), pp. 299–308
26. K.-H. Indlekofer, Remarks on an elementary proof of Halász's theorem. Lietuvos Mat. Rinkinys **33**(4), 417–423 (1993)
27. K.-H. Indlekofer, Number theory - probabilistic, heuristic and computational approaches. Comput. Math. Appl. **43**, 1035–1061 (2002)
28. K.-H. Indlekofer, New approach to probabilistic number theory. Theory Stoch. Process. **8**(24)(1–2), 136–153 (2002)
29. K.-H. Indlekofer, New approach to probabilistic number theory - compactifications and integration. Adv. Stud. Pure Math. **49**, 133–170 (2007)
30. K.-H. Indlekofer, On a quantitative form of Wirsing's mean-value theorem for multiplicative functions. Publ. Math. Debrecen **75**(1–2), 105–121 (2009)
31. K.-H. Indlekofer, A survey of Turán's equivalent power series, in *Number Theory, Analysis and Combinatorics, Proceedings of the Paul Turán Memorial Conference* Held August 22–26, 2011 in Budapest (De Gruyter, Berlin, 2014), pp. 127–143.
32. K.-H. Indlekofer, I. Kátai, On a theorem of H. Daboussi. Publ. Math. Debrecen **57**(1–2), 145–152 (2000)
33. K.-H. Indlekofer, I. Kátai, A note on a theorem of Daboussi. Acta Math. Hungar. **101**(3), 211–216 (2003)
34. K.-H. Indlekofer, E. Kaya, The three series theorem in additive arithmetical semigroups. Ann. Univ. Sci. Budapest. Sect. Comp. **38**, 201–220 (2012)
35. K.-H. Indlekofer, E. Manstavicius, New approach to multiplicative functions on arithmetical semigroups. Lietuvos Mat. Rinkinys **34**(4), 449–458 (1994)
36. K.-H. Indlekofer, E. Manstavicius, Translates of additive and multiplicative functions defined on arithmetical semigroups. Acta Sci. Math. **61**, 105–122 (1995)
37. K.-H. Indlekofer, R. Wagner, About positive linear functionals on spaces of arithmetical functions. Ann. Univ. Sci. Budapest. Sect. Comp. **40**, 295–306 (2013)
38. K.-H. Indlekofer, L.G. Lucht, J. Steuding, Obituary for Wolfgang Schwarz. Jahresber. Dtsch. Math.-Ver. **116**, 153–169 (2014)
39. K.-H. Indlekofer, E. Kaya, R. Wagner, Orthonormal systems in spaces of number theoretical functions (preprint)
40. J. Knopfmacher, *Abstract Analytic Number Theory* (North Holland, Amsterdam, 1975)
41. J. Knopfmacher, Fourier analysis of arithmetical functions. Ann. Mat. Pura Appl. (4) **109**, 177–201 (1976)

42. H. Kubota, H. Sugita, Probabilistic proof of limit theorems in number theory by means of adeles. Kyushu J. Math. **56**, 391–404 (2002)
43. L.G. Lucht, An application of Banach algebra techniques to multiplicative functions. Math. Z. **214**, 287–295 (1993)
44. L.G. Lucht, A survey of Ramanujan expansions. Int. J. Number Theory **6**, 1785–1799 (2010)
45. J. Mauclaire, *Integration et Theorie des Nombres* (Hermann, Paris, 1986)
46. H.L. Montgomery, R.C. Vaughan, Exponential sums with multiplicative coefficients. Inventiones Math. **43**, 69–82 (1977)
47. E.V. Novoselov, On a bicompact ring and its applications to number theory (in Russian), Izv. Akad. Nauk SSSR Ser. Mat. **28**, 307–364 (1964); English translation Am. Math. Sot. Transl. **52**(2) (1966)
48. E.V. Novoselov, A new method in probabilistic number theory. Izv. Akad. Nauk SSSR Ser. Mat. **28**, 307–364 (1964); English translation Am. Math. Soc. Transl. **52**(2) (1966)
49. H. Prüfer, Neue Begründung der algebraischen Zahlentheorie. Math. Ann. **94**, 198–243 (1925)
50. S. Ramanujan, On certain trigonometrical sums and their applications in the theory of numbers. Trans. Camb. Philos. Soc. **22**, 259–276 (1918) (Collected Papers, Cambridge 1927, No. 21)
51. W. Schwarz, Bemerkungen zu einem Satz der Herren Turán und Clunie über das Verhalten von Potenzreihen auf dem Rande des Konvergenzkreises. Publ. Math. Debrecen **16**, 67–73 (1969)
52. W. Schwarz, Bemerkungen zu einem Satz der Herren Turán und Clunie über das Verhalten von Potenzreihen auf dem Rande des Konvergenzkreises, II. Publ. Math. Debrecen **18**, 129–137 (1971)
53. W. Schwarz, Ramanujan-Entwicklungen stark multiplikativer zahlentheoretischer Funktionen. Acta Arith. **22**, 329–338 (1973)
54. W. Schwarz, Ramanujan-Entwicklungen stark multiplikativer Funktionen. J. Reine Angew. Math. **262/263**, 66–73 (1973)
55. W. Schwarz, Eine weitere Bemerkung über multiplikative Funktionen. Colloq. Math. **28**, 81–89 (1973)
56. W. Schwarz, Die Ramanujan-Entwicklung reellwertiger multiplikativer Funktionen vom Betrag kleiner oder gleich Eins. J. Reine Angew. Math. **271**, 171–176 (1974)
57. W. Schwarz, Über die Ramanujan-Entwicklung multiplikativer Funktionen. Acta Arith. **27**, 269–279 (1975)
58. W. Schwarz, Periodic, multiplicative number-theoretical functions. Monatshefte Math. **87**, 65–67 (1979)
59. W. Schwarz, Ramanujan expansions of arithmetical functions, in *Ramanujan Revisited, Urbana-Champaign IL*, 1987 (Academic, Boston, 1988), pp. 187–214
60. W. Schwarz, Some highlights from the history of probabilistic number theory, in *Proceedings of the International Conference on Probability and Number Theory, Kanazawa, 2005*. Advanced Studies in Pure Mathematics, vol. 49 (Math. Soc. Japan, Tokyo, 2007), pp. 367–419
61. W. Schwarz, J. Spilker, Eine Anwendung des Approximationssatzes von Weierstraß-Stone auf Ramanujan-Summen. Nieuw Archief voor Wisk. **19**(3), 198–209 (1971)
62. W. Schwarz, J. Spilker, *Arithmetical Functions: An Introduction to Elementary and Analytic Properties of Arithmetic Functions and to Some of Their Almost-Periodic Properties* (Cambridge University Press, Cambridge, 1994)
63. P. Turán, A remark concerning the behaviour of a power series on the periphery of its convergence circle. Publ. Inst. Math. (Belgr.) **12**, 19–26 (1958)
64. F. Tuttas, Über die Entwicklung multiplikativer Funktionen nach Ramanujan-Summen. Acta Arith. **36**, 257–270 (1980)
65. R. Warlimont, Ramanujan expansions of multiplicative functions. Acta Arith. **42**, 112–120 (1983)
66. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen II. Acta Math. Acad. Sci. Hung. **18**, 411–467 (1967)

On Some Selected Works of Wolfgang Schwarz

Aleksandar Ivić

Dedicated to the memory of Prof. Wolfgang Schwarz

Abstract In this overview paper, presented at the meeting ELAZ2014, Hildesheim, July 28–August 1, 2014, we present some selected works of the eminent mathematician Wolfgang Schwarz. This choice is personal and reflects the common research interest of the author and Prof. Schwarz.

Keywords Arithmetic functions • Asymptotic formulas • Riemann zeta-function • Tauberian theorems

2010 Mathematics subject classification: Primary 11N37; Secondary 11N45, 11N56, 11P82, 40E05

1 Introduction

Wolfgang Karl Schwarz (21 April 1934–19 July 2013) was a prolific and eminent German mathematician, working primarily in number theory. This paper presents some of his number-theoretic works, the choice being influenced by the common research interests of Prof. W. Schwarz and the author.

I had the pleasure of meeting W. Schwarz for the first time during the Oberwolfach meeting on "Elementary and Analytic Number Theory" in November 1980, although I started corresponding with him a few years before. W. Schwarz (together with H.-E. Richert and E. Wirsing) was one of the organizers of these Oberwolfach meetings at the "Mathematsches Forschungsinstitut" for many years.

Before I met him, we already wrote a joint paper on some number-theoretic equations (see [24] and Sect. 7.2). Definitely, Prof. Schwarz had a strong mathematical

A. Ivić (✉)
Serbian Academy of Science and Arts, Knez Mihailova 35, 11000 Beograd, Serbia
e-mail: aleksandar.ivic@rgf.bg.ac.rs; aivic_2000@yahoo.com

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_13

influence on me. For example, the paper [25] written jointly with E. Krätzel, M. Kühleitner, and W.G. Nowak was written after a suggestion from W. Schwarz. He had a vast mathematical culture, a clear and detailed style, and many mathematical subjects which interested him. Besides, he was a man of the world, a true gentleman indeed. He was also dedicated to mountain climbing, chess, and was a very fine musician; I am sure he could have made a very good professional career in music.

Wolfgang Schwarz was a prolific author, covering many fields of number theory. The Mathematical Reviews list more than 110 of his publications. These include

- Papers on arithmetic functions (multiplicative, additive, and particular)
- Papers involving prime numbers
- Papers on almost periodic and almost-even functions and related topics
- Tauberian theorems (with applications)
- Monographs
- Historical papers
- Textbooks
- Other works

The content of this paper covers roughly some of the topics mentioned above. This volume contains some other papers on the life and work of W. Schwarz, also presented at the Hildesheim ELAZ meeting in 2014. These are works by my friends and colleagues Indlekofer [15], Lucht [30], and Steuding [60]. These authors also recently published an obituary of Schwarz [16].

As to the quality of Schwarz's work, one could perhaps mention the excerpt from the review [MR2405612 (2009d:11001), A. Laurinčikas] of Schwarz's paper [45], "Some highlights from the history of probabilistic number theory": "...is an excellent survey on probabilistic number theory, with principal results and methods, and respective comments, accompanied by a list of more than 250 references and by photos of some of the mathematicians mentioned."

The last time I saw W. Schwarz was during the meeting "ELAZ2012" ("Elementare und Analytische Zahlentheorie," at Schloß Schney (Bavaria), August 13–18, 2012. He gave there a brilliant talk on the famous mathematician Theodor Schneider (1911–1988), and the mathematical life in Germany in the 1930s. Without passing judgements, he described in detail (with photos, documents, etc.) the turbulent times of Germany in the 1930s and the different fates of some mathematicians. This was his last public appearance. He died on July 19, 2013. With his passing the number-theoretic community, especially the German one, has lost one of its most distinguished members.

2 On Some Arithmetic Functions

W. Schwarz has written numerous important papers on arithmetic functions, especially on almost periodic and almost-even functions and related topics (see, e.g., the papers [48, 51, 52, 55–57] and [39] for some of the more recent works

on this subject which Schwarz wrote alone or with other authors). This, however, falls outside the scope of this paper. Here we shall analyze some of his works on particular arithmetic functions, although many papers have to be omitted, like the works on "B-Zwillinge" (numbers n such that both n and $n+1$ are a sum of two integral squares) [17] (with K.-H. Indlekofer) and [46]. We begin with some of W. Schwarz's work from 1960 to 1970.

2.1 The Euler Function

In [40] W. Schwarz obtains asymptotic formulae for the sums

$$\sum_{n\leqslant x}\varphi\big(f(n)\big),\quad \sum_{p\leqslant x}\varphi\big(f(p)\big),$$

where

$$\varphi(m)=m\prod_{p\mid m}\left(1-\frac{1}{p}\right)=\sum_{n\leqslant m,(n,m)=1}1$$

is Euler's (totient) function, p denotes primes, and

$$f(n)=a_0n^k+\cdots+a_k\ (>0)$$

is a polynomial (primitive, i.e., $(a_0,a_1,\ldots,a_k)=1$) with integer coefficients and discriminant $D>0$. In the paper he has ten lemmas (one is the Siegel–Walfisz form of the prime number theorem) and six theorems. For example, he also proves ($\omega(n)=\sum_{p\mid n}1=$ number of distinct prime factors of n) the asymptotic formulas

$$\sum_{p\leqslant x}\omega\big(f(p)\big)=\frac{x}{\log x}\cdot\log\log x+O\left(\frac{x\log\log\log x}{\log x}\right)$$

$$\sum_{n\leqslant x,\mu(n)\neq0}\omega\big(f(n)\big)=\frac{6}{\pi^2}x\log\log x+O(x),$$

where the condition $\mu(n)\neq0$ ($\mu(n)$ is the Möbius function) means that the last sum is over square-free numbers. One notes at once that there are several footnotes in the text. Footnotes are definitely a trademark of Schwarz's mathematical style, and he was fond of using them! For example, on page 50 he has the definition of a strongly additive function as "Footnote No. 3":

[3] $F(n)$ heißt stark additiv, wenn für teilerfremde Zahlen n_1,n_2, stets $F(n_1n_2)=F(n_1)+F(n_2)$ gilt und für jede ganze Zahl $r\geqslant1$ stets $F(p^r)=F(p)$ ist.

3 Tauberian Theorems

3.1 Habilitationsschrift

Tauberian theorems (Alfred Tauber, 1866–1942) are (partial) converses of abelian theorems (Niels Henrik Abel, 1802–1829). Namely, if the series $\sum\limits_{n=0}^{\infty} a_n$ converges to A, then Abel proved that

$$\lim_{x\to 1-0}\sum_{n=0}^{\infty} a_n x^n = A.$$

Tauber [61] in 1897 proved, if $na_n = o(1)$ as $n \to \infty$, then the converse is also true. The qualifying Tauberian hypothesis "$na_n = o(1)$" can be relaxed to $a_n = O(1/n)$, say by Hardy–Littlewood [7, 8]. The Habilitationsschrift [41] of W. Schwarz uses Tauberian theorems of Hardy–Littlewood [7, 8], Hardy–Ramanujan [9, 10], Ikehara [14], Ingham [18], Karamata [26, 27], Martin–Pitt–Wiener (see [31, 34, 35]), and a host of other methods and results.

For an extensive account on Tauberian theorems, see the monograph [28] of Jacob Korevaar. The Habilitationsschrift [41], in published form [42], is perhaps Schwarz's most comprehensive and deepest work. It deals primarily with the evaluation of the summatory function

$$\sum_{n\leqslant x} f(n) \tag{3.1}$$

for multiplicative functions $f(n)$ ($f(mn) = f(m)f(n)$ for $(m,n) = 1$), under the assumption that

$$\sum_{p\leqslant x} f(p)\log p = Kx\log^{\alpha} x + R(x),$$

and $R(x)$ (= "Restglied") is the remainder term. The asymptotic evaluation of (3.1) is one of the most fundamental problems in the theory of arithmetic functions.

The case $\alpha \leqslant 0$ was settled by E. Wirsing [62] in 1961 by intricate methods, but here also the (more difficult) case $\alpha > 0$ is considered. Briefly, the multiplicativity of $f(n)$ leads to the Euler product representation

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_{p}\left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots\right) \quad (\mathrm{Re}\, s > 1).$$

A Tauberian theorem of Hardy and Ramanujan [9, 10] gives first an evaluation for

$$\log\left\{\sum_{n\leqslant x} f(n)\right\}.$$

Ingham's Tauberian theorem [18] gives then $\sum_{n\leqslant x} f(n)/n$. Finally an idea of E. Wirsing produces an evaluation of $\sum_{n\leqslant x} f(n)$. The assumptions are: $R(x) = O(x), f(p) = o(p\log^{-\alpha-1} p), f(p^k) \leqslant \gamma p^{k-1-\delta}k^{-2}$ for some $\delta > 0$ and $k \geqslant 2$.

3.2 Applications of Tauberian Theorems

The dissertation is essentially published in three important works [42], Part A, B, and C. Part B brings forth the asymptotic formula for

$$P(x) := \sum_{n\leqslant x} \frac{1}{\alpha(n)}, \quad \alpha(n) = \prod_{p|n} p,$$

so that the multiplicative function $\alpha(n)$ is the square-free kernel of n. It was shown by de Bruijn [5] (see also his monograph [4]) that

$$\log P(x) \sim \sqrt{8}(\log x/\log\log x)^{1/2} \qquad (x\to\infty).$$

The asymptotic formula for $P(x)$ itself is harder! By using Ingham's Tauberian theorem Schwarz obtained a true asymptotic formula for $P(x)$. This is

$$P(x) = (4\pi)^{-1/2}2^{-1/4}\left(\frac{\log\log x}{\log x}\right)^{1/2} Q(x), \tag{3.2}$$

where

$$Q(x) := \min_{0<\sigma<\infty} x^{\sigma}\sum_{n=1}^{\infty}\frac{1}{\alpha(n)n^{\sigma}}.$$

One can put (3.2) into another form: as $x\to\infty$

$$P(x) = \frac{1+o(1)}{\sqrt{4\pi\sqrt{2}}}\left(\frac{\log\log x}{\log x}\right)^{1/4}\exp\Big(-\mathcal{R}(\log x)\Big),$$

where

$$-\mathcal{R}(u) \sim 2\sqrt{2}\sqrt{\frac{u}{\log u}} \qquad (u\to\infty).$$

These problems involve a detailed study of the asymptotic behavior of the generating function

$$\varphi(s) := \sum_p \log\left(1 + \frac{1}{p(p^s - 1)}\right),$$

since

$$\mathcal{F}(s) = \exp\bigl(\varphi(s)\bigr), \quad \mathcal{F}(s) = \sum_{n=1}^{\infty} \frac{1}{\alpha(n) \cdot n^s} \quad (\mathrm{Re}\, s > 0).$$

Several other results on $\alpha(n)$ are also proved, e.g.,

$$\sum_{n \leqslant x} \frac{n}{\alpha(n)} = o\left(x \sum_{n \leqslant x} \frac{1}{\alpha(n)}\right) \quad (x \to \infty).$$

In Part C [42] of his "Habilitationsschrift" Schwarz considers the so-called Mahler's problem from the theory of partitions. Namely, let

$$0 < \lambda_1 < \lambda_2 < \cdots, \quad \sum_{\lambda_\nu \leqslant u} 1 = B \log^\beta u + O(1),$$

where $B > 0, 0 < \beta \leqslant 1$. For $\mathrm{Re}\, s > 0$ let

$$\prod_{\nu=1}^{\infty} \bigl\{1 - \exp\bigl(-\lambda_\nu s\bigr)\bigr\}^{-1} = \exp\Bigl(\phi(s)\Bigr),$$

say. Further, let σ_u denote the positive solution of $-\phi'(\sigma_u) = u$, and $T(u) = \phi(\sigma_u) + u\sigma_u$, and let $P(u)$ denote the number of solutions of the inequality

$$n_1\lambda_1 + n_2\lambda_2 + \cdots < u$$

in non-negative integers n_ν. Schwarz proves that, as $u \to \infty$,

$$P(u) \ \sim \ \bigl\{2\pi B \log^\beta u\bigr\}^{-1/2} \exp\bigl(T(u)\bigr).$$

4 Distribution of Values of Finite Abelian Groups

4.1 General

W. Schwarz published the works [43] on $a(n)$, the number of non-isomorphic abelian (commutative) groups of order n, plus the joint papers with Herzog [13] and Wirsing [58].

The function $a(n)$ is multiplicative and prime-independent, namely one has $a(p^\alpha) = P(\alpha)$, where $P(\alpha)$ is the number of unrestricted partitions of $\alpha \in \mathbb{N}$, hence $a(p) = 1, a(p^2) = 2, a(p^3) = 3, a(p^4) = 5$, etc. Let ($p$ denotes primes)

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1} \qquad (\mathrm{Re}\, s > 1),$$

be the familiar Riemann zeta-function, which possesses analytic continuation to $\mathbb{C}$ and is regular, except at $s = 1$ where it has a simple pole with residue 1. Then the generating series of $a(n)$ can be written as

$$\mathcal{A}(s) := \sum_{n=1}^{\infty} a(n) n^{-s} = \zeta(s)\zeta(2s)\zeta(3s)\ldots \qquad (\mathrm{Re}\, s > 1).$$

Therefore the Dirichlet series $\mathcal{A}(s)$ has poles at $s = 1/1, 1/2, 1/3, \ldots$, so that one expects the summatory function $A(x) := \sum_{n \leqslant x} a(n)$ to be well approximated by

$$\sum_j c_j x^{1/j}, \quad c_j := \prod_{k=1, k\neq j}^{\infty} \zeta\left(\frac{k}{j}\right).$$

Indeed, W. Schwarz in Part II of [43] shows that

$$A(x) - \sum_{j=1}^{6} c_j x^{1/j} = O(x^{1/6-\varepsilon}) \tag{4.1}$$

cannot hold for any given $\varepsilon > 0$.

4.2 Results on $\Delta(x)$

If we set

$$A(x) = \sum_{j=1}^{5} c_j x^{1/j} + \Delta(x),$$

then the author [22] showed that

$$\int_1^X \Delta^2(x)\, \mathrm{d}x \;=\; \Omega(X^{4/3} \log X),$$

where $f(x) = \Omega\Big(g(x)\Big)$ means $\lim_{x\to\infty} f(x)/g(x) \neq 0$. This gives a slight sharpening of (4.1), namely

$$\Delta(x) = \Omega\left(x^{1/6}\sqrt{\log x}\right).$$

In the other direction the author [21] showed that

$$\int_1^X \Delta^2(x)\,\mathrm{d}x = O(X^a \log^b X) \qquad (a = 39/29 = 1.34482\ldots), \tag{4.2}$$

and Heath-Brown [11] obtained the mean square formula with $a = 4/3$ and $b = 89$. In view of the Omega-result for $\Delta(x)$ the exponent 4/3 in (4.2) is best possible.

Open problems: is it true that

$$\int_1^X \Delta^2(x)\,\mathrm{d}x = (C + o(1))X^{4/3} \qquad (C > 0,\ X \to \infty)?$$

Can one evaluate the higher moments of $\Delta(x)$?

There is a rich history on upper bounds for $\Delta(x)$, starting from the seminal paper of Erdős and Szekeres [6] in 1935, who obtained $\Delta(x) = O(\sqrt{x})$. Sharpening a method of Richert [37] who established

$$\Delta(x) = O(x^{3/10}\log^{9/10} x), \tag{4.3}$$

W. Schwarz in Part I of [43] obtained (4.3) with the better exponent of x (stated by Schwarz as his "Satz 3" in this way!)

$$\frac{3}{10} - \frac{7}{30\cdot 23}.$$

H.-E. Richert actually conjectured that

$$\Delta(x) = o(x^{1/4}) \qquad (x \to \infty), \tag{4.4}$$

which is quite deep and does not seem to be within reach yet. All recent results on upper bounds for $\Delta(x)$ were obtained by estimating exponential sums connected with the error term in the asymptotic formula for $\sum\limits_{ab^2c^3\leqslant x} 1$ (see, e.g., Chap. 14 of [23]).

4.3 The Order of $\Delta(x)$ and $a(n)$

The best known result on the upper bound for $\Delta(x)$, proved decades later in 2006, comes relatively close to (4.4). Namely, Robert and Sargos [38] proved that

$$\Delta(x) \;=\; O_\varepsilon\left(x^{1/4+\varepsilon}\right).$$

Here O_ε (and $\ll_\varepsilon$ below) means that the implied O-constant depends only on ε, which is an arbitrarily small, positive number. The crucial bound used in their proof, which is actually best possible, has an arithmetical flavor. It says that

$$\mathcal{N} \ll_\varepsilon (N^4\delta + N^2) \qquad (\delta > 0),$$

where $\mathcal{N}$ is the number of integer quadruples (m, n, k, ℓ) such that $N < m, n, k, \ell \leqslant 2N$ and

$$|\sqrt{m} + \sqrt{n} - \sqrt{k} - \sqrt{\ell}| < \delta\sqrt{N}.$$

The maximal order of $a(n)$ is considered in Schwarz and Wirsing in [58]. The minimal order of $a(n)$ is trivial, since $a(p) = 1$ $(\forall p)$. Sharpening a result of E. Krätzel [29] they prove, as $n \to \infty$,

$$\log a(n) \leqslant \log 5 \cdot \operatorname{li}\left(\frac{1}{4}\log n\right) + O\left\{\log n \cdot \exp\left(-c_1\sqrt{\log\log n}\right)\right\},$$

where $c_1 > 0$ and

$$\operatorname{li} x \;=\; \int_2^x \frac{1}{\log t}\,\mathrm{d}t.$$

Also, there are infinitely many values of n such that $(c_2 > 0)$

$$\log a(n) \geqslant \log 5 \cdot \operatorname{li}\left(\frac{1}{4}\log n\right) + O\left\{\log n \cdot \exp\left(-c_2\sqrt{\log\log n}\right)\right\},$$

so that the upper and lower bound for $a(n)$ are of the same form. Generalizations to multiplicative, prime-independent functions of these results have been obtained by Heppner [12], Nicolas [32, 33], and others.

5 Distribution of Values of the Omega Functions

In [45], W. Schwarz investigated the so-called Rényi's problem (Alfred Rényi, 1921–1970, a well-known Hungarian mathematician after whom the Mathematical Institute in Budapest is named). Let $\mathcal{K}$ be the set of numbers $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ such that $\alpha_1 + \dots + \alpha_r - r = 1$, or equivalently $\Omega(n) - \omega(n) = 1$, where

$$\Omega(n) = \sum_{p^\alpha \| n} \alpha, \qquad \omega(n) = \sum_{p|n} 1.$$

Thus $\Omega(n)$ is the number of all prime factors of n, multiplicities counted, while $\omega(n)$ denotes the number of distinct prime factors of n. One also defines $\Omega(1) = \omega(1) = 0$. Rényi's problem consists of the estimation of the counting function

$$K(x) = \sum_{n \leqslant x, n \in \mathcal{K}} 1 = \sum_{n \leqslant x, \Omega(n) - \omega(n) = 1} 1.$$

Rényi [36] in 1955 proved that

$$K(x) = \frac{6}{\pi^2} \alpha x + o(x) \qquad \left(\alpha = \sum_p \frac{1}{p(p+1)},\ x \to \infty \right).$$

Cohen [1, 2] improved this to

$$K(x) = \frac{6}{\pi^2} \alpha x + O(x^{1/2} \log\log x).$$

W. Schwarz obtained, for any fixed $r \in \mathbb{N}$,

$$K(x) = \frac{6}{\pi^2} \alpha x + \frac{\sqrt{x}}{\log x} \sum_{k=0}^{r-1} b_k \log^{-k} x + O\left(\frac{\sqrt{x}}{\log x} \log^{-r} x \right),$$

where the constants b_k are explicitly given. Dieter Wolke [63] in 1991 considered the more general problem of the estimation of

$$F_q(x) := \sum_{n \leqslant x, \Omega(n) - \omega(n) = q} 1,$$

where $q \in \mathbb{N}$ is given (so that $K(x) \equiv F_1(x)$). His result improves the results of Schwarz on $K(x)$. It says that for explicit $d_k > 0$ ($d_1 = 6\pi^{-2}\alpha$),

$$F_q(x) = d_q x + \\ + x^{1/2} \sum_{1 \leqslant j \leqslant N(x)} P_{j,q}(\log\log x)(\log x)^{-j-1} \\ + O\left\{x^{1/2}\exp(-b_2 N(x))\right\}.$$

Here $N(x) = \log^{1/3} x(\log\log x)^{-1/3}$. The polynomials $P_{j,q}(x)$ (of degree $\leqslant q-1$) satisfy

$$|P_{j,q}(\log\log x)| \leqslant b_3 b_4^j (j+1)! q \log x \quad (b_3 > 0,\ b_4 > 0),$$

which is an explicit bound.

6 Schwarz on the History of Primes

W. Schwarz has written many remarkable review papers, textbooks, and monographs. For some of them, see [47–50, 53, 54, 56, 59]. I have particularly liked his textbook [47], "Einführung in die Zahlentheorie." It deals with many classical subjects of number theory, but Schwarz manages to present them in a novel and interesting way. His paper [50] on the history of primes is a real *tour de force*, analyzing superbly many topics connected with prime numbers. But let me refer to the review of the paper by D.R. Heath-Brown:

MR1298643 (95h:11001)

> This is a comprehensive survey of the history of the prime number theorem and of developments from it. It makes inspiring reading, describing numerical investigations, a wide range of different proofs of the prime number theorem, and a whole range of other prime number theory, including primes in arithmetic progressions, sieve methods, and additive prime number theory. There are a number of photographs of researchers in the area, and occasional quotations from original papers, giving the article a down-to-earth feel. Overall this is an excellent read for any mathematician.

7 Schwarz's Influence on the Author

W. Schwarz influenced me in more ways than one. We had many common interests in multiplicative number theory. I began corresponding with him in 1975, and the contact lasted even after he was seriously ill in 2012. The last e-mail message I received from him was a Christmas greeting in December 2012. Most of all, I remember his gentlemanly figure and his vast mathematical culture during the

many Oberwolfach meetings on "Elementary and Analytic Number Theory" at the Mathematisches Forschungsinstitut, which he organized for several decades together with H.-E. Richert and E. Wirsing. I owe very much to all three of them, especially to Schwarz, for being regularly invited there, as these meetings enabled me to meet most of the contemporary important research workers in analytic number theory, to mention just P. Erdős, Matti Jutila, and Y. Motohashi, with all of whom I have later collaborated extensively. I am taking the liberty to conclude this paper with two specific examples of W. Schwarz's influence on me.

7.1 Numbers of the Form pr^2

Around 1975 I came to the paper of Schwarz [44] on the distribution of numbers of the form pr^2, where p is prime, and $r \in \mathbb{N}$. I was a beginner in analytic number theory in those days. The proof of Schwarz's result was not difficult, and the paper was written very clearly, so it immediately appealed to me. Let

$$C(x) \ = \sum_{pr^2 \leqslant x} 1$$

denote the number of integers of the form pr^2 not exceeding x. Schwarz used a nice elementary argument to show that, for a fixed integer $k \geqslant 0$,

$$C(x) = \sum_{n=0}^{k} C_n x(\log x)^{-n-1} + O\left(x(\log x)^{-k-2}\right),$$

where

$$C_0 = \pi^2/6 = \zeta(2),\ C_n = (-2)^n \zeta^{(n)}(2) + nC_{n-1} \quad (n \geqslant 1).$$

As soon as I read the paper, it occurred to me that Schwarz's argument can be readily generalized to a somewhat more general situation. I wrote a short paper, which was published in the Polish periodical "Colloquium Mathematicum" (see [20]), the same journal in which Schwarz's paper was published. It was, quite appropriately, reviewed by W. Schwarz himself, who in MR0498446 said verbatim:

Using Dirichlet's trick of splitting double sums carefully, the author proves a general theorem which gives an asymptotic formula for the number of integers $n \leqslant x$ of the form $n = a \cdot b$, where $a \in \mathcal{A}, b \in \mathcal{B}$, under the assumption that an asymptotic formula is given for the counting function $B(x) = \sum_{b \leqslant x, b \in \mathcal{B}} 1$ and that an estimate

$$A(x) = \sum_{a \leqslant x, a \in \mathcal{A}} 1 \ = \ O(x^c)$$

is known, where $0 < c < 1$. *As a special case this theorem contains the asymptotic formula*

$$\sum_{pr^2 \leqslant x} 1 = \sum_{n=0}^{k} C_n x(\log x)^{-n-1} + O\left(x(\log x)^{-k-2}\right).''$$

It is fairly obvious that my work was not of a high quality, but Schwarz did not want to discourage me, so he did not express any explicit criticism. In fact, it was he who suggested that I submit the paper to "Colloquium Mathematicum," and his advice was always sound and well-intended.

7.2 Number-Theoretical Equations

In [19] I solved a system of number-theoretic equations involving the number of divisors function $d(n)$. I simultaneously published the problem in the "American Mathematical Monthly" as Problem 6108. This asked to find all multiplicative functions $f(n)$ for which

$$f(n^2) = \sum_{d|n} \mu^2(d) f\left(\frac{n}{d}\right)$$

and

$$f^2(n) = \sum_{d|n} f(d^2).$$

W. Schwarz contacted me soon afterwards with some ideas on how to generalize this problem. This led to our joint paper [24].

Let

$$(f * g)(n) := \sum_{d|n} f(d)g(n/d), \quad (f \perp g)(n) := \sum_{d|n,(d,n/d)=1} f(d)g(n/d),$$

denote the Dirichlet convolution and unitary convolution of $f(n)$ and $g(n)$, respectively. These arithmetic operations were studied extensively in the 1960s and 1970s by many authors, e.g., see Eckford Cohen [1], [3].

Several number-theoretic equations involving Dirichlet and unitary convolution are discussed in [24]. One of the basic problems is the analysis of the equation

$$f^k = 2^\omega * f \qquad (k = 1, 2, \cdots). \tag{7.1}$$

If $k = 1$, the only non-negative solution of (7.1) satisfying $f(1) = 1$ is the divisor function $f(n) = d(n)$. If $k \geqslant 3$ is odd [resp. $k \geqslant 2$ is even] there exists exactly one real-valued [resp. non-negative] function f satisfying (7.1) and $f(1) = 1$. In both cases the solution f is multiplicative and prime-independent (meaning $f(p^\alpha) = g(\alpha)$, in other words $f(p^\alpha)$ does not depend on α). The analogues for the unitary convolution are also discussed in the paper.

References

1. E. Cohen, Unitary functions (mod r). Duke Math. J. **28**, 475–485 (1961) and II. Publ. Math. Debrecen **9**, 94–104 (1962)
2. E. Cohen, Arithmetical notes VIII. An asymptotic formula of A. Rényi. Proc. Am. Math. Soc. **13**, 536–539 (1962)
3. E. Cohen, Some asymptotic formulas in the theory of numbers. Trans. Am. Math. Soc. **112**, 214–227 (1964)
4. N.G. de Bruijn, *Asymptotic Methods in Analysis, Bibliotheca Mathematica*, vol. 4 (North-Holland Publishing, Amsterdam; P. Noordhoff Ltd., Groningen; Interscience Publishers, New York, 1958), xii+200 pp.
5. N.G. de Bruijn, On the number of integers $\leqslant x$ whose prime factors divide n. Illinois J. Math. **6**, 137–141 (1962)
6. P. Erdős, G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. Acta Sci. Math. (Szeged) **7**, 95–102 (1935)
7. G.H. Hardy, J.E. Littlewood, Tauberian theorems concerning power series and Dirichlet series whose coefficients are positive. Proc. Lond. Math. Soc. (2) **13**, 174–191 (1914)
8. G.H. Hardy, J.E. Littlewood, Abel's theorem and its converse. Proc. Lond. Math. Soc. (2) **18**, 205–235 (1918), and II. ibid., **22**, 254–269 (1923).
9. G.H. Hardy, S. Ramanujan, Asymptotic formulae for integers of various types. Proc. Lond. Math. Soc. (2) **16**, 112–132 (1917)
10. G.H. Hardy, S. Ramanujan, Asymptotic formulae in combinatorial analysis. Proc. Lond. Math. Soc. (2) **17**, 75–115 (1918)
11. D.R. Heath-Brown, The number of abelian groups of order at most x, Journées Arithmétiques, 1989 (Luminy, 1989). Astérisque No. **198–200**(1991), 153–163 (1992)
12. E. Heppner, Die maximale Ordnung primzahl-unabhängiger multiplikativer Funktionen. Arch. Math. **24**, 63–66 (1973)
13. J. Herzog, W. Schwarz, Über eine spezielle Partitionenfunktion, die mit der Anzahl der abelschen Gruppen der Ordnung n zusammenhängt. Analysis **5**(1–2), 153–161 (1985)
14. S. Ikehara, An extension of Landau's theorem in the analytic theory of numbers. J. Math. Phys. (Mass. Inst. of Technology) **10**, 1–12 (1931)
15. K.-H. Indlekofer, Arithmetical functions - a pivotal topic in the scientific work of Wolfgang Schwarz, in *From Arithmetic to Zeta-Functions. Number Theory in Memory of Wolfgang Schwarz* (Springer, Cham, 2016), pp. 179–199
16. K.-H. Indlekofer, L.G. Lucht, J. Steuding, Obituary for Wolfgang Schwarz. Jahresber. Dtsch. Math.-Ver. **116**(3), 153–169 (2014)
17. K.-H. Indlekofer, W. Schwarz, Über B-Zwillinge. Arch. Math. **23**, 251–256 (1972)
18. A.E. Ingham, On Wiener's method in Tauberian theorems. Proc. Lond. Math. Soc. (2) **38**, 458–480 (1935)
19. A. Ivić, On a number-theoretical system of functional equations. Rev. Res. Sci. Univ. Novi Sad **6**, 1–5 (1976)
20. A. Ivić, A theorem in asymptotic number theory. Colloq. Math. **39**(1), 177–184 (1978)

21. A. Ivić, The number of finite non-isomorphic abelian groups in mean square. Hardy-Ramanujan J. **9**, 17–23 (1986)
22. A. Ivić, The general divisor problem. J. Number Theory **27**, 73–91 (1987)
23. A. Ivić, *The Riemann-Zeta Function* (Wiley, New York, 1985) (2nd edn., Dover, Mineola, 2003)
24. A. Ivić, W. Schwarz, Remarks on some number-theoretical functional equations. Aequationes Math. **20**, 80–89 (1980)
25. A. Ivić, E. Krätzel, M. Kühleitner, W.G. Nowak, Lattice points in large regions and related arithmetic functions: recent developments in a very classic topic, in *Proceedings ELAZ-Conference*, May 24–28, 2004, ed. by W. Schwarz, J. Steuding (Franz Steiner Verlag, Stuttgart, 2006), pp. 89–128
26. J. Karamata, Über die Hardy-Littlewoodschen Umkehrungen des Abelschen Stetigkeitssatzes. Math. Zeit. **32**(1), 319–320 (1930)
27. J. Karamata, Neuer Beweis und Verallgemeinerung einiger Tauberian-Sätze, Math. Zeit. **33**(1), 294–299 (1931)
28. J. Korevaar, *Tauberian Theorems - A Century of Developments*. Grundlehren der Math. Wissenschaften, vol. 320 (Springer, Berlin, 2004)
29. E. Krätzel, Die maximale Ordnung der Anzahl der wesentlich verschiedenen abelschen Gruppen n-ter Ordnung. Quart. J. Math. Oxford Ser. (2) **21**, 273–275 (1970)
30. L. Lucht, Remembering Wolfgang Schwarz, his life and work, in *From Arithmetic to Zeta-Functions. Number Theory in Memory of Wolfgang Schwarz* (Springer, Cham, 2016), pp. 247–261
31. W.T. Martin, N. Wiener, Taylor's series of functions of smooth growth in the unit circle. Duke Math. J. **4**, 384–392 (1938)
32. J.-L. Nicolas, Grandes valeurs des fonctions arithmétiques, Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 2, Exp. No. G20, 5 pp. Secrétariat Mathématique, Paris, 1975
33. J.-L. Nicolas, Grandes valeurs d'une certaine classe de fonctions arithmétiques. Studia Sci. Math. Hungar. **15**(1–3), 71–77 (1980)
34. H.R. Pitt, General Tauberian theorems. Proc. Lond. Math. Soc. **44**, 243–288 (1938) and II, J. Lond. Math. Soc. **15**, 97–112 (1940)
35. H.R. Pitt, *Tauberian Theorems* (Oxford University Press, Oxford, 1958)
36. A. Rényi, On the density of certain sequences of integers. Acad. Serbe Sci. Publ. Inst. Math. **8**, 157–162 (1955)
37. H.-E. Richert, Über die Anzahl Abelscher Gruppen gegebener Ordnung I. Math. Z. **56**, 21–32 (1952) and II, ibid., **8**, 71–84 (1953)
38. O. Robert, P. Sargos, Three-dimensional exponential sums with monomials. J. Reine Angew. Math. **591**, 1–20 (2006)
39. J.-C. Schlage-Puchta, W. Schwarz, J. Spilker, Uniformly-almost-even functions with prescribed values. IV. Application of Gelfand theory. Analysis **24**(1), 63–70 (2004)
40. W. Schwarz, Über die Summe $\sum_{n\leqslant x} \varphi(f(n))$ und verwandte Probleme. Monatsh. Math. **66**, 43–54 (1962)
41. W. Schwarz, Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. Habilitationsschrift vorgelegt zur Erlangung der venia legendi für Mathematik der Hohen Naturwissenschaftlich-Mathematischen Fakultät der Albert-Ludwigs-Universität zu Freiburg i. Br. Dissertation, Freiburg, 1964, xviii+103 pp.
42. W. Schwarz, Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. Part A. J. Reine Angew. Math. **219**, 67–96 (1965), Part B. ibid., 157–179, Part C, Mahler's Partitions problem, ibid. **228**, 182–188 (1967)
43. W. Schwarz, Über die Anzahl Abelscher Gruppen gegebener Ordnung. I Math. Z. **92**, 314–320 (1966) und II, J. Reine Angew. Math. **228**, 133–138 (1967)
44. W. Schwarz, Eine Bemerkung über die Anzahl der Zahlen pr^2 unterhalb x. Colloq. Math. **19**, 117–120 (1968)

45. W. Schwarz, Eine Bemerkung zu einer asymptotischen Formel von Herrn Rényi. (German). Arch. Math. (Basel) **21**, 157–166 (1970)
46. W. Schwarz, Über *B*-Zwillinge. II. Arch. Math. (Basel) **23**, 408–409 (1972)
47. W. Schwarz, *Einführung in die Zahlentheorie*, 2nd edn. (Die Mathematik. Wissenschaftliche Buchgesellschaft, Darmstadt, 1987), xii+274 pp.
48. W. Schwarz, *Ramanujan Expansions of Arithmetical Functions. Ramanujan Revisited (Urbana-Champaign, IL, 1987)* (Academic, Boston, MA, 1988), pp. 187–214
49. W. Schwarz, Geschichte der analytischen Zahlentheorie seit 1890, Ein Jahrhundert Mathematik 1890–1990, 741–780, Dokumente Gesch. Math., 6, Vieweg, Braunschweig, 1990
50. W. Schwarz, *Some Remarks on the History of the Prime Number Theorem from 1896 to 1960*. Development of Mathematics 1900–1950 (Luxembourg, 1992) (Birkhäuser, Basel, 1994), pp. 565–616
51. W. Schwarz, Uniform-fast-gerade Funktionen mit vorgegebenen Werten. Arch. Math. **77**(1), 1–4 (2001)
52. W. Schwarz, John Knopfmacher, [abstract] analytic number theory, and the theory of arithmetical functions. Dedicated to the memory of John Knopfmacher. Quaest. Math. **24**(3), 273–290 (2001)
53. W. Schwarz, Some highlights from the history of probabilistic number theory, in *Probability and Number Theory–Kanazawa 2005*. Advanced Studies in Pure Mathematics, vol. 49 (Mathematical Society of Japan, Tokyo, 2007), pp. 367–419
54. W. Schwarz, 40 puzzles and problems in probability and mathematical statistics, in *Problem Books in Mathematics* (Springer, New York, 2008), xii+124 pp.
55. W. Schwarz, J. Spilker, Mean values and Ramanujan expansions of almost even arithmetical functions, in *Topics in Number Theory (Proc. Colloq., Debrecen, 1974)*. Colloq. Math. Soc. Janos Bolyai, vol. 13 (North-Holland, Amsterdam, 1976), pp. 315–357
56. W. Schwarz, J. Spilker, Arithmetical functions, in *An Introduction to Elementary and Analytic Properties of Arithmetic Functions and to Some of their Almost-Periodic Properties*. London Mathematical Society Lecture Note Series, vol. 184 (Cambridge University Press, Cambridge, 1994), xx+367 pp.
57. W. Schwarz, J. Spilker, Uniform-fast-gerade Funktionen mit vorgegebenen werten. II. Arch. Math. **81**(5), 534–537 (2003)
58. W. Schwarz, E. Wirsing, The maximal number of non-isomorphic abelian groups of order *n*. Arch. Math. **24**, 59–62 (1973)
59. W. Schwarz, W. Wolfart, J. Vorwort, Zur Geschichte des Mathematischen Seminars der Universität Frankfurt am Main von 1914 bis heute, Aus der Geschichte der Frankfurter Mathematik, 8-133, Schr. Universitätsarchivs Frankf. am Main, 1, Universitätsarchiv Frankf. am Main, Frankfurt am Main, 2005
60. J. Steuding, On Liouville numbers - yet another application of functional analysis to number theory, in *From Arithmetic to Zeta-Functions. Number Theory in Memory of Wolfgang Schwarz* (Springer, Cham, 2016), pp. 485–507
61. A. Tauber, Ein Satz aus der Theorie der unendlichen Reihen. Monatsh. F. Math. **8**, 273–277 (1897)
62. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. Math. Ann. **143**, 75–102 (1961)
63. D. Wolke, On a problem of A. Rényi. Monatsh. Math. **111**(4), 323–330 (1991)

Sums of Two Squares of Sums of Two Squares

Rebecca Ulrike Jakob

Dedicated to Wolfgang Schwarz

Abstract This article determines the order of magnitude of integers not exceeding x that can be written as sums of two squares of integers that are themselves sums of two squares. The tools include Selberg's sieve and contour integration in the spirit of the Selberg-Delange method.

Keywords Arithmetic progression • Square • Sum • Sums of two squares

2010 Mathematics subject classification: Primary 11N36; Secondary 11M99

1 Introduction

In about 1900 Landau calculated the cardinality of sums of two squares in a long interval $[1, x]$. With $\mathcal{S} = \{n \in \mathbb{N} \mid n = a^2 + b^2\}$ he proved in [3] the asymptotic formula

$$\sum_{\substack{n \le x \\ n \in \mathcal{S}}} 1 = C \frac{x}{\sqrt{\log x}} + \mathcal{O}\left(\frac{x}{(\log x)^{3/2}}\right), \tag{1.1}$$

where $C := \frac{1}{\sqrt{2}} \prod_{p \equiv 3(4)} (1 - p^{-2})^{-1/2}$.

It is possible to diversify the summation condition in a lot of ways. In this paper we want to consider the situation where each of the two squares is again a sum of two squares.

R.U. Jakob (✉)
Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany
e-mail: r.jakob@stud.uni-goettingen.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_14

We define some notation. Let $\tilde{\mathcal{S}} = \{n \in \mathbb{N} \mid p|n \Rightarrow p \not\equiv 3(4)\} \subset \mathcal{S}$, and let

$$R(n) = \#\{a, b \in \mathcal{S} \mid n = a^2 + b^2\},$$
$$\tilde{R}(n) = \#\{a, b \in \tilde{\mathcal{S}} \mid n = a^2 + b^2\}.$$

Finally we write

$$S_i(x) = \sum_{n \le x} R(n)^i$$

for $i = 0, 1, 2$ with the convention $0^0 = 0$, and analogously

$$\tilde{S}_i(x) = \sum_{n \le x} \tilde{R}(n)^i.$$

Our aim is to estimate these quantities from above and below. We start with the following which can be obtained from (1.1) by partial summation.

Theorem 1.1 *For $x \ge 3$ we have the asymptotic formula*

$$S_1(x) = \frac{\pi}{4} \prod_{p \equiv 3(4)} (1 - p^{-2})^{-1} \frac{x}{\log x} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big).$$

An analogous asymptotic formula (with a different constant) can be proved for $\tilde{S}_1(x)$.

Our next aim is an upper bound for $\tilde{S}_2(x)$. As a preparation we define the function

$$\varphi_s(n) := \prod_{p|n} \big(1 - p^{-s}\big). \tag{1.2}$$

Then we prove the following

Theorem 1.2 *Let $q_j,\ r_j \in \mathbb{Z}$ for $j = 1, \dots, k$ with $\mathcal{Q} = \prod_j q_j \prod_{i \ne j} |q_i r_j - q_j r_i| \ne 0$. Then*

$$\#\{n \le x \mid q_j n + r_j \in \tilde{\mathcal{S}}\ \forall j = 1, \dots, k\}$$
$$\le \frac{x}{(\log x)^{k/2}} \frac{\Gamma(k/2+1) 2^k}{F^k(1)} \frac{1}{\varphi_1^k(\mathcal{Q})} \bigg(1 + \mathcal{O}\Big(\Big(\frac{\log \mathcal{Q}}{\varphi_1^k(\mathcal{Q})} + \varphi_{1-\delta'}^{-2k}(\mathcal{Q})\Big) \frac{1}{\log x}\Big)\bigg),$$

for a constant $\delta' > 0$ and $F^k(1)$ given by the convergent Euler product

$$\prod_p \Big(1 - \frac{\chi_{-4}(p)}{p}\Big)^{k/2} \prod_{p \equiv 3(4)} \Big(1 + \sum_{l=2}^{k} \binom{k}{l} p^{-l}\Big)\big(1 - p^{-2}\big)^{-k/2}.$$

This furnishes an upper bound for numbers such that k arithmetic progressions are not divisible by a prime congruent to 3 modulo 4.

To prove this theorem we use Selberg's sieve which requires a calculation that is reminiscent of the Selberg-Delange method. Having this bound available, we will prove the following theorem.

Theorem 1.3 *For $x \geq 3$ we have the upper bound*

$$\tilde{S}_2(x) \ll \frac{x}{\log x}. \tag{1.3}$$

We see that $\tilde{S}_1(x)$ and $\tilde{S}_2(x)$ have the same order of magnitude, thus with the Cauchy-Schwarz inequality we get a good lower bound for $\tilde{S}_0(x)$. Furthermore we have the inequality $\tilde{S}_0(x) \leq S_0(x)$, so we get a lower bound for $S_0(x)$. This gives us our final result.

Theorem 1.4 *For $x \geq 3$ we have*

$$\frac{x}{\log x} \ll S_0(x) \leq C_o \frac{x}{\log x}\Big(1 + \mathcal{O}\Big(\frac{1}{\log x}\Big)\Big)$$

with $C_o = \frac{\pi}{4} \prod_{p \equiv 3(4)} (1 - p^{-2})^{-1}$.

In other words, the number of sums of two squares of sums of two squares is of order of magnitude $\frac{x}{\log x}$.

2 Useful Lemmas

First we will prove three lemmas which are useful to prove the theorems.

Lemma 2.1 *For fixed $n, m \in \mathbb{N}$ we get*

$$-\int_0^{\sqrt{x}} \frac{t}{\sqrt{\log t}^m} \frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)}^n}\Big)dt = \frac{\sqrt{2}^m \pi}{4} \frac{x}{\sqrt{\log x}^{n+m}}\Big(1 + \mathcal{O}\Big(\frac{1}{\log x}\Big)\Big).$$

Proof Let $X = \frac{\sqrt{x}}{(\log x)^{(m+n+2)/2}}$. We consider the two integrals over $[0, X]$ and $[X, \sqrt{x}]$ separately, and denote them by $I_e(x)$ and $I_m(x)$, respectively.

In the integrand of $I_e(x)$ the derivative is bounded by

$$\frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)}^n}\Big) \ll \frac{X}{\sqrt{x-X^2}\sqrt{\log(x-X^2)}^n} \ll \frac{X}{\sqrt{x-X^2}}.$$

Using this and the estimate $\frac{t}{\sqrt{\log t}^m} \ll X$ we obtain

$$I_e(x) \ll \int_0^X \frac{X^2}{\sqrt{x-X^2}}dt \ll \frac{X^3}{\sqrt{x}} \ll \frac{x}{(\log x)^{(m+n+2)}}.$$

For the integrand of $I_m(x)$ we use Taylor's formula around $t = \sqrt{x}$

$$\frac{1}{\sqrt{\log t}^m} = \frac{\sqrt{2}^m}{\sqrt{\log x}^m} + \mathcal{O}\Big(\frac{t-\sqrt{x}}{\sqrt{x}\sqrt{\log x}^{m+2}}\Big).$$

For the integral over the error term we compute the derivative term and use trivial bounds for the factors

$$\int_X^{\sqrt{x}} \frac{(\sqrt{x}-t)t^2}{\sqrt{x-t^2}\sqrt{\log(x-t^2)}^n}|n-\log(x-t^2)^{-1}|dt\frac{1}{\sqrt{x}\sqrt{\log x}^{m+2}} \ll \frac{x}{\sqrt{\log x}^{m+n+2}}.$$

In the remaining integral for the main term $\big(\frac{2}{\log x}\big)^{m/2}$ of Taylor's formula we expand the lower bound to zero. With partial integration and the substitution $y = x - t^2$ we get an integral similar to the one above, whence

$$\int_X^{\sqrt{x}} t\frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)}^n}\Big)dt = \int_0^x \frac{\sqrt{y}}{2\sqrt{x-y}\sqrt{\log y}^n}dy + \mathcal{O}\Big(\frac{x}{\sqrt{\log x}^{n+2}}\Big).$$

We need to compute the integral. Again we split it into two parts $[0, Z]$ and $[Z, x]$ with $Z = \frac{x}{(\log x)^{n/2+1}}$ and repeat the estimates to get

$$\int_0^x \frac{\sqrt{y}}{2\sqrt{x-y}\sqrt{\log y}^n}dy = \frac{1}{\sqrt{\log x}^n}\int_0^x \frac{\sqrt{y}}{2\sqrt{x-y}}dy\Big(1+\mathcal{O}\Big(\frac{1}{\log x}\Big)\Big).$$

The remaining integral $\int_0^x \frac{\sqrt{y}}{\sqrt{x-y}}dy$ can be computed exactly with the result $\frac{x\pi}{2}$ and our claim follows.

Lemma 2.2 *The map*

$$\{(k,l,m,n) \in \mathbb{N}^4 \mid kl = mn\} \longleftrightarrow \{(s,t,u,v) \in \mathbb{N}^4 \mid (s,u) = 1\},$$
$$(k,l,m,n) \longmapsto \Big(\frac{k}{(k,m)}, (k,m), \frac{m}{(k,m)}, \frac{n(k,m)}{k}\Big),$$
$$(st, uv, tu, sv) \longmapsfrom (s,t,u,v)$$

is a bijection.

The proof is straightforward.

Lemma 2.3 *Let $k \in \mathbb{N}$ and $s > 1/2$. Then for $x \geq 3$ we have*

$$\sum_{n \leq x} \frac{1}{n} \varphi_s^{-k}(n) \ll \log x.$$

Proof The case $s = 1$ and $k = 1$ was proved by Landau (c.f. [2]). Note that $n\varphi_1(n)$ is Euler's phi function.

The expression $\frac{1}{\varphi_s(n)}$ can be rewritten as

$$\frac{1}{\varphi_s(n)} = \prod_{p|n} \big(1 - \frac{1}{p^s}\big)^{-1} = \prod_{p|n} \big(1 + \frac{1}{p^s - 1}\big) = \sum_{d|n} \frac{\mu^2(d)}{d^s \varphi_s(d)}$$

where μ is the Möbius function. We insert this in our summation to get

$$\begin{aligned}
\sum_{n \leq x} \frac{1}{n} \varphi_s^{-k}(n) &= \sum_{n \leq x} \frac{1}{n} \Big(\sum_{d|n} \frac{\mu^2(d)}{d^s \varphi_s(d)} \Big)^k \\
&= \sum_{\substack{d_j \leq x \\ j=1,\dots,k}} \frac{\mu^2(d_1) \cdots \mu^2(d_k)}{d_1^s \varphi_s(d_1) \cdots d_k^s \varphi_s(d_k)} \frac{1}{\operatorname{lcm}_i(d_i)} \sum_{m \leq \frac{x}{\operatorname{lcm}_i(d_i)}} \frac{1}{m} \\
&\ll \sum_{\substack{d_j \leq x \\ j=1,\dots,k}} \Big| \frac{\mu^2(d_1) \cdots \mu^2(d_k)}{d_1^s \varphi_s(d_1) \cdots d_k^s \varphi_s(d_k)} \Big| \frac{1}{\operatorname{lcm}_i(d_i)} \cdot \log x.
\end{aligned}$$

We complete the remaining sum into an infinite sum and see

$$\sum_{\substack{d_j = 1 \\ j=1,\dots,k}}^{\infty} \Big| \frac{\mu^2(d_1) \cdots \mu^2(d_k)}{d_1^s \varphi_s(d_1) \cdots d_k^s \varphi_s(d_k)} \Big| \frac{1}{\operatorname{lcm}_i(d_i)} \ll \prod_p \Big(1 + \frac{1}{p(p^s - 1)} \Big)^k.$$

This product converges absolutely for $s > 1/2$.

3 Numbers in $\tilde{\mathcal{S}}$ in Arithmetic Progressions

In this section we prove Theorem 1.2. For simplification we assume $k \geq 2$, since in the case $k = 1$ we can apply the proof of (1.1) with a different constant. In addition, if (q_j, r_j) has a divisor which is congruent to 3 (mod 4) there are no solutions, hence the inequality is true. If (q_j, r_j) has a prime divisor $p \equiv 1 \pmod 4$, we can simply divide it out without changing the condition $q_j n + r_j \in \tilde{\mathcal{S}}$. Hence we assume without

loss of generality that $(q_j, r_j) = 1$. We use Selberg's sieve, c.f. [1, Theorem 6.4, p. 10]. Let

$$\mathcal{P} = \prod_{\substack{p \equiv 3(4) \\ k < p \le x}} p \qquad \text{and}$$

$$Q(t) = (q_1 t + r_1) \dots (q_k t + r_k).$$

Then the cardinality of $\{n \le x \mid (Q(n), \mathcal{P}) = 1\}$ is an upper bound for the quantity we want to bound.

Consider the function $\rho(d) = \#\{a \pmod d \mid Q(a) \equiv 0 \pmod d\}$. We see that $\rho(p) \le \min\{k, p\}$ for $p \mid \mathcal{P}$. In particular it is $\rho(p) = k$ if $(p, \mathcal{Q}) = 1$. By the Chinese remainder theorem, ρ is multiplicative. Hence we get

$$\sum_{\substack{n \le x \\ d \mid Q(n)}} 1 = \frac{x}{d}\rho(d) + \mathcal{O}(\tau_{k-1}(d)),$$

where τ_k is the k-th iterated divisor function $\sum_{a_1 \cdots a_k = n} 1$.

We define the multiplicative function g by $g(p) = \frac{\rho(p)}{p - \rho(p)}$ for primes $p \mid \mathcal{P}$, $g(p) = 0$ for $p \nmid \mathcal{P}$ and $g(p^\nu) = 0$ for all p and all $\nu \ge 2$. For a parameter z to be chosen later let $Z = \sum_{d \le z} g(d)$. Therefore by Selberg's sieve

$$\sum_{\substack{n \le x \\ (Q(n), \mathcal{P}) = 1}} 1 \le \frac{x}{Z} + \mathcal{O}\Big(\sum_{\substack{d \le z^2 \\ p \mid \mathcal{P}}} \tau_3(d)\tau_{k-1}(d) \Big). \tag{3.1}$$

Hence we need to find a lower bound for Z to get the information we want. Writing

$$Z' = \sum_{d \le z} \mu^2(d) \prod_{\substack{p \mid d \\ p \mid \mathcal{Q} \\ p \equiv 3(4)}} g(p) \prod_{\substack{p \mid d \\ p \nmid \mathcal{Q} \\ p \equiv 3(4)}} \frac{\tau_{k-1}(p)}{p},$$

it is easy to see that $Z \ge Z'$.

For the sum Z' we use Perron's formula to find a lower bound. It will be useful to use a refined version due to Liu and Ye [4]. Consider the Dirichlet series of Z', given by the Euler product

$$\begin{aligned} D(s) :&= \prod_{\substack{p \mid \mathcal{Q} \\ p \equiv 3(4) \\ p > k}} \Big(1 + \frac{g(p)}{p^s}\Big)\Big(1 + \frac{\tau_{k-1}(p)}{p^{s+1}}\Big)^{-1} \prod_{p \equiv 3(4)} \Big(1 + \frac{\tau_{k-1}(p)}{p^{s+1}}\Big) \\ &= D'(s) \cdot \zeta^{k/2}(s+1) L^{-k/2}(s+1, \chi_{-4}) H(s), \end{aligned}$$

where

$$D'(s) = \prod_{\substack{p\mid\mathcal{Q}\\ p\equiv 3(4)\\ p>k}} \big(1+\frac{g(p)}{p^s}\big)\big(1+\frac{\tau_{k-1}(p)}{p^{s+1}}\big)^{-1}.$$

The function $H(s)$ is holomorphic and nonzero in $\operatorname{Re} s > -\frac{1}{2}$. The finite product $D'(s)$ also is a holomorphic function and bounded by

$$\varphi_{1+\operatorname{Re} s}^{2k}(\mathcal{Q}) \ll \big|D'(s)\big| \ll \frac{1}{\varphi_{1+\operatorname{Re} s}^{2k}(\mathcal{Q})},$$

where φ_s is as in (1.2). Define $F^2(s+1) = \zeta(s+1)L^{-1}(s+1,\chi_{-4})H^{2/k}(s)s$, then F is holomorphic in the zero-free region of the L-function as in [6, II §5.4] and we get $D(s) = F^k(s+1)s^{-k/2}D'(s)$.

Let $2 \le T < z$ be a parameter which we choose later. For the error terms in Perron's formula we need to bound the quantity

$$\begin{aligned}\sum_{|z-n|\le \frac{z}{\sqrt{T}}} g(n) &\ll \sum_{|z-n|\le \frac{z}{\sqrt{T}}} \mu^2(n)\tau_{k-1}(n) \prod_{\substack{p\mid n\\ k<p,p\mid\mathcal{Q}}} \frac{1}{p-k} \prod_{\substack{p\mid n\\ p\nmid\mathcal{Q}}} \frac{1}{p}\\ &\ll \varphi_1^{-k}(\mathcal{Q}) \sum_{|z-n|\le \frac{z}{\sqrt{T}}} \mu^2(n)\frac{\tau_{k-1}(n)}{n} \ll \varphi_1^{-k}(\mathcal{Q})\frac{(\log(z))^{k-2}}{\sqrt{T}}.\end{aligned}$$

The last bound follows by [5, Theorem 2]. The second part of the error term is given by

$$\frac{z^b B(b)}{\sqrt{T}} \ll \frac{z^b}{\sqrt{T}} \sum_n \frac{|g(n)|}{n^b} \ll \frac{\zeta^k(1+\frac{1}{\log z})}{\sqrt{T}} \ll \frac{(\log z)^k}{\sqrt{T}},$$

where we choose $b = \frac{1}{\log z}$.

By applying Perron's formula in the version of [4, Corollary 2.2] we get

$$Z' = \frac{1}{2\pi i}\int_{\frac{1}{\log z}-iT}^{\frac{1}{\log z}+iT} \frac{F^k(s+1)}{s^{k/2}} D'(s) z^s \frac{ds}{s} + \mathcal{O}\Big(\varphi_1^{-k}(\mathcal{Q})\frac{(\log(z))^{k-2}}{\sqrt{T}} + \frac{(\log z)^k}{\sqrt{T}}\Big). \tag{3.2}$$

Now we integrate over the same contour as in Tenenbaum [6, II §5.4] but shifted to zero, so that the order of the singularity at 0 is $\frac{k}{2}+1$.

We split the contour into various pieces

$$\begin{aligned}
\gamma_1, \gamma_7 &= \Big[c \mp iT, -\frac{\delta}{2\log(2+T)} \mp iT\Big],\\
\gamma_2, \gamma_6 &= -\frac{\delta}{2\log(2+|t|)} + it, \text{for } t \in [-T, 0], t \in [0, T],\\
\gamma_4 &= \partial B_r(0),\\
\gamma_3 &= \Big[-\frac{\delta}{2\log 2}, -r\Big],\\
\gamma_5 &= \Big[-r, -\frac{\delta}{2\log 2}\Big],
\end{aligned}$$

with $r = \frac{1}{\log z}$ and $\delta > 0$ is chosen so small that

$$\frac{1}{L(s, \chi_{-4})} \ll \log|t|, \qquad \zeta(s) \ll \log|t|,$$

for $\sigma > 1 - \frac{\delta}{2\log(2+|t|)}$ (see [6, p. 262]).

For the parts γ_i with $i = 1, 2, 6, 7$ an upper bound for $D'(s)$ is given by the function $\varphi_{1-\delta'}^{-2k}(\mathcal{Q})$ with $\delta' = \frac{\delta}{2\log 2}$. We get for γ_1 and analogously for γ_7 the bound

$$\begin{aligned}
\int_{\gamma_1} \frac{F^k(s+1)}{s^{k/2}} D'(s) z^s \frac{ds}{s} &\ll \frac{(\log T)^k}{\varphi_{1-\delta'}^{2k}(\mathcal{Q})} \int_{-\frac{\delta}{2\log(2+T)}}^{\frac{1}{\log z}} z^\sigma \frac{d\sigma}{T}\\
&\ll \varphi_{1-\delta'}^{-2k}(\mathcal{Q}) \frac{(\log T)^k}{T} \int_{-\frac{\delta}{2\log(2+T)}}^{\frac{1}{\log z}} z^\sigma d\sigma \ll \varphi_{1-\delta'}^{-2k}(\mathcal{Q}) \frac{(\log T)^k}{T}.
\end{aligned} \tag{3.3}$$

For the parts γ_2 and γ_6 the bound is given by

$$\begin{aligned}
&\int_{\gamma_2} \frac{F^k(s+1)}{s^{k/2}} D'(s) z^s \frac{ds}{s}\\
&\ll \varphi_{1-\delta'}^{-2k}(\mathcal{Q}) (\log T)^k z^{-\delta/(2\log T)} \int_0^T \Big|\frac{\delta}{2\log T} - it\Big|^{-1} dt\\
&\ll \varphi_{1-\delta'}^{-2k}(\mathcal{Q}) z^{-\delta/(2\log T)} \frac{2(\log T)^{1+k}}{\delta}.
\end{aligned} \tag{3.4}$$

We choose $T = \exp(\frac{\delta}{2}\sqrt{\log z})$ to optimize the error term composed from (3.2), (3.3) and (3.4).

By writing $\Upsilon' = \gamma_3\gamma_4\gamma_5$ for the contribution not yet considered we get with the bounds from (3.2), (3.3) and (3.4) the asymptotic formula

$$Z' = \frac{1}{2\pi i}\int\limits_{\Upsilon'} \frac{F^k(s+1)}{s^{k/2}} D'(s) z^s \frac{ds}{s} + \mathcal{O}\Big(\big(\varphi_{1-\delta'}^{-2k}(\mathcal{Q}) + \varphi_1^{-k}(\mathcal{Q})\big)\frac{(\log z)^k}{\exp(\delta\sqrt{\log z})}\Big). \tag{3.5}$$

The remaining integral does not have an explicit solution, but by using the Taylor expansion

$$F^k(s+1)D'(s) = F^k(1)D'(0) + \mathcal{O}\Big(\varphi_1^{-k}(\mathcal{Q})\log\mathcal{Q}\cdot|s|\Big)$$

we obtain

$$\Big|\frac{1}{2\pi i}\int\limits_{\Upsilon'} \frac{F^k(s+1)}{s^{k/2}} D'(s) z^s \frac{ds}{s}\Big|$$

$$\geq \varphi_1^k(\mathcal{Q})F^k(1)\Big|\frac{1}{2\pi i}\int\limits_{\Upsilon'} s^{-k/2} z^s \frac{ds}{s}\Big| + \mathcal{O}\Big(\varphi_1^k(\mathcal{Q})\log\mathcal{Q}\Big|\int\limits_{\Upsilon'} \frac{|s|}{s^{k/2}} z^s \frac{ds}{s}\Big|\Big) = I_h(z) + I_e(z).$$

The product $D'(0)$ is bounded from below by $\varphi_1^k(\mathcal{Q})$. Now we change $I_h(z)$ by the substitution $s = \frac{w}{\log z}$ into the form of Theorem 5.2 from [6, II §5.2]. Let Υ be the resulting contour from Υ'. Applying Corollary 2.1 of [6, II §5.2], for Hankel's contour we get

$$\begin{aligned} I_h(z) &\geq F^k(1)\varphi_1^k(\mathcal{Q})(\log z)^{k/2}\Big|\frac{1}{2\pi i}\int\limits_{\Upsilon} e^w w^{-(k/2+1)} dw\Big| \\ &= F^k(1)\varphi_1^k(\mathcal{Q})(\log z)^{k/2}\Big(\frac{1}{\Gamma(k/2+1)} + \mathcal{O}(z^{-\nu})\Big), \end{aligned}$$

for some $\nu > 0$.

To compute the integral $I_e(z)$ we use trivial bounds on the circle and on the lines separately to get $I_e \ll \varphi_1^{-k}(\mathcal{Q})\log\mathcal{Q}(\log z)^{k/2-1}$. Combining the obtained results we get a lower bound for Z' and hence for Z. The error terms from Perron's formula and from the other pieces of the contour (3.5) combine with $I_e(x)$ to give

$$\begin{aligned} &\varphi_1^{-k}(\mathcal{Q})\log\mathcal{Q}(\log z)^{k/2-1} + \big(\varphi_{1-\delta'}^{-2k}(\mathcal{Q}) + \varphi_1^{-k}(\mathcal{Q})\big)\frac{(\log z)^k}{\exp(\delta\sqrt{\log z})} \\ &\ll \big(\varphi_1^{-k}(\mathcal{Q})\log\mathcal{Q} + \varphi_{1-\delta'}^{-2k}(\mathcal{Q})\big)(\log z)^{k/2-1}. \end{aligned} \tag{3.6}$$

The error terms in Eqs. (3.1) and (3.6) are optimized by choosing $z = \frac{x^{1/2}}{(\log x)^d}$ with $d = \frac{1}{2}(\frac{k}{2} + 1 + 3^k)$ and we get

$$\begin{aligned}&\#\{n \le x \mid q_j n + r_j \in \tilde{\mathcal{S}}\ \forall j = 1, \dots, k\}\\ &\le \frac{x}{(\log x)^{k/2}} \frac{\Gamma(k/2+1)2^{k/2}}{F^k(1)} \frac{1}{\varphi_1^k(\mathcal{Q})}\Big(1 + \mathcal{O}\Big(\Big(\frac{\log \mathcal{Q}}{\varphi_1^k(\mathcal{Q})} + \varphi_{1-\delta'}^{-2k}(\mathcal{Q})\Big)\frac{1}{\log x}\Big)\Big).\end{aligned}$$

4 Proof of Theorem 1.1

In this section we find an asymptotic formula for $S_1(x)$.

Let $r_0(n)$ be the characteristic function on the numbers that can be written as a sum of two squares. By rewriting the sum in terms of $r_0(n)$ and (1.1) we get

$$S_1(x) = \sum_{a \le \sqrt{x}} r_0(a) C \frac{\sqrt{2}\sqrt{x-a^2}}{\sqrt{\log(x-a^2)}}\Big(1 + \mathcal{O}\big((\log(x-a^2))^{-1}\big)\Big).$$

By applying partial summation and once more (1.1) we get the integrals

$$\begin{aligned}S_1(x) =& -C^2\sqrt{2}\int_0^{\sqrt{x}} \frac{t}{\sqrt{\log t}} \frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)}}\Big)dt\\ &+ \sum_{n \le \sqrt{x}} r_0(n) \lim_{a \to \sqrt{x}} \frac{\sqrt{x-a^2}}{\sqrt{\log(x-a^2)}}\big(1 + \frac{1}{\log(x-a^2)}\big)\\ &+ \mathcal{O}\Big(\int_0^{\sqrt{x}} \frac{t}{\sqrt{\log t^3}} \frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)}}\Big)dt + \int_0^{\sqrt{x}} \frac{t}{\sqrt{\log t}} \frac{d}{dt}\Big(\frac{\sqrt{x-t^2}}{\sqrt{\log(x-t^2)^3}}\Big)dt\Big)\\ =:& M(x) + 0 + E(x).\end{aligned}$$

The boundary expression vanishes since $\lim_{a \to \sqrt{x}} \frac{\sqrt{x-a^2}}{\sqrt{\log(x-a^2)}}\big(1 + (\log(x-a^2))^{-1}\big) = 0$.

With Lemma 2.1 at our disposal the computation of $M(x)$ and $E(x)$ is simple.

For $M(x)$ we have $m = n = 1$ and hence

$$M(x) = C^2\sqrt{2}\frac{\sqrt{2}\pi}{4}\frac{x}{\log x} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big).$$

The error term $E(x)$ has two integrals, where in the first one we have $m = 3$, $n = 1$ and in the second one $m = 1$, $n = 3$. Since Lemma 2.1 is symmetric in n and m it yields $E(x) \ll \frac{x}{(\log x)^2}$.

Combining these two terms we conclude that

$$S_1(x) = C^2 \frac{\pi}{2} \frac{x}{\log x} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big). \tag{4.1}$$

The asymptotic formula for $\tilde{S}_1(x)$ is almost the same as $S_1(x)$, and for $x \geq 3$ we get

$$\tilde{S}_1(x) = \frac{\pi}{4} \prod_{p \equiv 3(4)} (1 - p^{-2}) \frac{x}{\log x} + \mathcal{O}\Big(\frac{x}{(\log x)^2}\Big).$$

5 Proof of Theorem 1.3

The upper bound of $\tilde{S}_2(x)$ requires a bit more work. Opening the square we have

$$\tilde{S}_2(x) = \sum_{\substack{a,b,c,d \in \tilde{\mathcal{S}} \\ a^2+b^2=c^2+d^2 \leq x}} 1.$$

We need to understand the summation condition $a^2 + b^2 = c^2 + d^2$. The diagonal term is $\tilde{S}_1(x)$ which we have bound above. Hence we can assume that $\{a, b\} \neq \{c, d\}$ and the condition $a^2 + b^2 = c^2 + d^2$ is equivalent to $(a+d)(a-d) = (c+b)(c-b)$. Using Lemma 2.2 this can be rewritten with $s, t, u, v \in \mathbb{N}$ with $(s, u) = 1$ as

$$a + d = st, \quad a - d = uv, \quad c + b = tu, \quad c - b = sv.$$

Without loss of generality we can assume that $a > b$ and $c > d$, then the condition $a, b, c, d \in \tilde{\mathcal{S}}$ changes to $st + uv$, $st - uv$, $ut + sv$, $ut - sv \in \tilde{\mathcal{S}}$. It follows that

$$\tilde{S}_2(x) \leq \sum_{\substack{st,uv,ut,sv \leq 2\sqrt{x} \\ st \pm uv, ut \pm sv \in \tilde{\mathcal{S}}}} 1.$$

Now we want to apply Theorem 1.2. We fix u, t, v and think of s as our variable. In accordance with Theorem 1.2, we define $\mathcal{Q} = tv(t - v)(t + v)(t^2 + v^2)$.

In the case $t = v$ our conditions imply that $t(s \pm u) > 0$ and $t(u \pm s) > 0$ which is obviously impossible.

In the following let $t \neq v$, so that $\mathcal{Q} \neq 0$. Isolating the sum over s we get

$$\sum_{\substack{st,uv,ut,sv \leq 2\sqrt{x} \\ st \pm uv, ut \pm sv \in \tilde{\mathcal{S}}}} 1 = \sum_{tu,uv \leq 2\sqrt{x}} \sum_{\substack{s \leq \min\{\frac{ut}{v}, \frac{2\sqrt{x}}{t}, \frac{2\sqrt{x}}{v}\} \\ st \pm uv, ut \pm sv \in \tilde{\mathcal{S}}}} 1.$$

We use Theorem 1.2 to calculate the inner sum, and obtain

$$\sum_{\substack{s\le\min\{\frac{ut}{v},\frac{2\sqrt{x}}{t},\frac{2\sqrt{x}}{v}\}\\ st\pm uv,ut\pm sv\in\mathcal{S}}} 1 \ll \frac{ut}{v}\frac{1}{(\log\frac{ut}{v})^2}\frac{1}{\varphi_1^4(\mathcal{Q})}\Big(1+\Big(\frac{\log\mathcal{Q}}{\varphi_1^4(\mathcal{Q})}+\varphi_{1-\delta'}^{-8}(\mathcal{Q})\Big)\frac{1}{\log\frac{ut}{v}}\Big),$$

with δ' defined in Sect. 3. For the sum over t,u,v we get the condition $v<t$, since $\frac{uv}{t}<\frac{ut}{v}$. Furthermore in the term $\varphi_1^4(\mathcal{Q})$ we split the product $\mathcal{Q}$. To this end a short look at the definition shows that $\varphi_s(nm)\ge\varphi_s(n)\varphi_s(m)$ and with the Hölder inequality it follows that

$$\begin{aligned}&\sum_{\substack{uv<ut\\ ut<2\sqrt{x}}}\frac{ut}{v}\frac{1}{(\log\frac{ut}{v})^2}\Big(\frac{1}{\varphi_1(t)}\frac{1}{\varphi_1(v)}\frac{1}{\varphi_1(t-v)}\frac{1}{\varphi_1(t+v)}\frac{1}{\varphi_1(t^2+v^2)}\Big)^4\\ &\ll\Big(\sum_{\substack{uv<ut\\ ut<2\sqrt{x}}}\frac{ut}{v}\frac{1}{(\log\frac{ut}{v})^2}\frac{1}{\varphi_1^{20}(v)}\Big)^{4/5}\Big(\sum_{\substack{u<2\sqrt{x}\\ n<\frac{2x}{u^2}}}\frac{u}{(\log u)^2}\frac{r(n)}{\varphi_1^{20}(n)}\Big)^{1/5},\end{aligned}\tag{5.1}$$

where $r(n)$ counts the number of solutions $a^2+b^2=n$.

First we compute the sum over v and use $(\log\frac{ut}{v})^{-2}<(\log u)^{-2}$. Using Lemma 2.3 to compute the remaining sum over v we get

$$\sum_{ut\le2\sqrt{x}}\sum_{v\le t}\frac{ut}{v}\frac{1}{(\log u)^2}\frac{1}{\varphi_1^4(v)}\ll\sum_{ut\le2\sqrt{x}}\frac{u}{(\log u)^2}t\log t.$$

With partial integration we get for the sum over $t\log t$ the upper bound

$$\sum_{t\le\frac{2\sqrt{x}}{u}}t\log t\ll\frac{x}{u^2}\Big(\log\frac{2\sqrt{x}}{u}-1\Big).$$

There remains the sum over u for which once again we use partial summation. We obtain

$$\sum_{u\le2\sqrt{x}}\frac{1}{u(\log u)^2}\log\frac{2\sqrt{x}}{u}\ll\frac{1}{\log x}.$$

Hence the first factor of (5.1) is computed.

Using $r(n)=\sum_{d|n}\chi_{-4}(d)$ the second factor of (5.1) can be transformed similarly as in Lemma 2.3 and it follows that

$$\sum_{n\le\frac{2x}{u^2}}\frac{r(n)}{\varphi_1^{20}(n)}\ll\frac{x}{u^2}.$$

And the sum over u can be computed as above to get

$$\sum_{\substack{u<2\sqrt{x}\\ n<2\frac{x}{u^2}}} \frac{u}{(\log u)^2}\frac{r(n)}{\varphi_1^{20}(n)} \ll \frac{x}{\log x}.$$

Combining these two results we get

$$\sum_{\substack{uv<ut\\ ut<2\sqrt{x}}} \frac{ut}{v}\frac{1}{(\log \frac{ut}{v})^2}\frac{1}{\varphi_1^4(\mathcal{Q})} \ll \frac{x}{\log x}.$$

For the sums over $\frac{\log \mathcal{Q}}{\varphi_1^4(\mathcal{Q})}$ and $\varphi_{1-\delta'}^{-8}(\mathcal{Q})$ the argument is the same and it follows in the same way that

$$\sum_{uv<ut<2\sqrt{x}} \frac{ut}{v}\frac{1}{(\log \frac{ut}{v})^3}\frac{\log \mathcal{Q}}{\varphi_1^8(\mathcal{Q})} \ll \sum_{uv<ut<2\sqrt{x}} \frac{ut}{v}\frac{1}{(\log \frac{ut}{v})^3}\frac{\log t}{\varphi_1^8(\mathcal{Q})} \ll \frac{x}{\log x}$$

and

$$\sum_{uv<ut<2\sqrt{x}} \frac{ut}{v}\frac{1}{(\log \frac{ut}{v})^3}\varphi_{1-\delta'}^{-8}(\mathcal{Q})\varphi_1^{-4}(\mathcal{Q}) \ll \frac{x}{(\log x)^2}.$$

Combining these two results we get the final bound

$$\tilde{S}_2(x) \ll \frac{x}{\log x}.$$

6 Final Result

Theorem 1.4 is now a consequence of the Cauchy-Schwarz inequality. We have

$$\tilde{S}_1(x) \le \Big(\sum_{n\le x}\tilde{R}(n)^0\Big)^{1/2}\Big(\sum_{n\le x}\tilde{R}(n)^2\Big)^{1/2} = \tilde{S}_0(x)^{1/2}\tilde{S}_2(x)^{1/2}.$$

Thus

$$S_0(x) \ge \tilde{S}_0(x) \ge \frac{\tilde{S}_1^2(x)}{\tilde{S}_2(x)}.$$

By replacing $\tilde{S}_2(x)$ with (1.3) and $\tilde{S}_1(x)$ with (4.1) we get the lower bound stated in Theorem 1.4.

On the other hand we have $S_0(x) \le S_1(x)$, which yields the upper bound.

Acknowledgements I am very grateful to Prof. Valentin Blomer for suggesting this topic to me and his constant advice and encouragement.

References

1. H. Iwaniec, E. Kowalski, *Analytic Number Theory*. American Mathematical Society Colloquium Publications, vol. 53 (American Mathematical Society, Providence, 2004)
2. E. Landau, Über die Zahlentheoretische Funktion φ(n) und ihre Beziehung zum Goldbachschen Satz. Nachr. Ges. Wiss. Goettingen, Math.-Phys. Kl. **1900**, 177–186 (1900)
3. E. Landau, Über die Zerlegung der Zahlen in zwei Quadrate. Annali di Matematica **20**(1), 1–28 (1913)
4. J. Liu, Y. Ye, Perron's formula and the prime number theorem for automorphic *L*-functions. Pure Appl. Math. Q. **3**(2), 481–497 (2007)
5. P. Shiu, A Brun-Titschmarsh theorem for multiplicative functions. J. Reine Angew. Math. **313**, 161–170 (1980)
6. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*. Cambridge Studies in Advanced Mathematics (Cambridge University Press, Cambridge, 1995)

The Joint Discrete Universality of Periodic Zeta-Functions

Antanas Laurinčikas

To the memory of Professor Wolfgang Schwarz

Abstract In the paper, a joint discrete universality theorem on approximation of a pair of analytic functions by shifts of periodic zeta-functions and periodic Hurwitz zeta-functions is obtained. For the proof the linear independence over $\mathbb{Q}$ of a certain set is used.

Keywords Algebraically independent numbers • Joint universality • Linear independence • Periodic Hurwitz zeta-function • Periodic zeta-function • Weak convergence

2010 Mathematics subject classification: Primary 11M41; Secondary 32E30

1 Introduction

Let $s = \sigma + it$ be a complex variable, and $\mathfrak{a} = \{a_m : m \in \mathbb{N}\}$ and $\mathfrak{b} = \{b_m : m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}\}$ be two periodic sequences of complex numbers with minimal periods $k \in \mathbb{N}$ and $l \in \mathbb{N}$, respectively. The periodic zeta-function $\zeta(s; \mathfrak{a})$ and periodic Hurwitz zeta-function $\zeta(s, \alpha; \mathfrak{b})$ with parameter α, $0 < \alpha \leq 1$, are defined, for $\sigma > 1$, by the series

$$\zeta(s; \mathfrak{a}) = \sum_{m=1}^{\infty} \frac{a_m}{m^s} \quad \text{and} \quad \zeta(s, \alpha; \mathfrak{b}) = \sum_{m=0}^{\infty} \frac{b_m}{(m+\alpha)^s}.$$

A. Laurinčikas (✉)
Department of Mathematics and Informatics, Vilnius University, Naugarduko str. 24, LT-03225 Vilnius, Lithuania
e-mail: antanas.laurincikas@maf.vu.lt

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_15

Let $\zeta(s,\alpha)$ denote the classical Hurwitz zeta-function which is for $\sigma > 1$ given by

$$\zeta(s,\alpha) = \sum_{m=0}^{\infty} \frac{1}{(m+\alpha)^s},$$

and can be analytically continued to the whole complex plane, except for a simple pole at the point $s = 1$ with residue 1. In view of the periodicity of the sequences $\mathfrak{a}$ and $\mathfrak{b}$, we have that, for $\sigma > 1$,

$$\zeta(s;\mathfrak{a}) = \frac{1}{k^s} \sum_{m=1}^{k} a_m \zeta\left(s, \frac{m}{k}\right)$$

and

$$\zeta(s,\alpha;\mathfrak{b}) = \frac{1}{l^s} \sum_{m=0}^{l-1} b_m \zeta\left(s, \frac{m+\alpha}{l}\right).$$

Thus, by the above remark on the function $\zeta(s,\alpha)$, these equalities give analytic continuation for the functions $\zeta(s;\mathfrak{a})$ and $\zeta(s,\alpha;\mathfrak{b})$ to the whole complex plane, except for a hypothetical simple pole at $s = 1$ with residues

$$a = \frac{1}{k} \sum_{m=1}^{k} a_m \quad \text{and} \quad b = \frac{1}{l} \sum_{m=0}^{l-1} b_m,$$

respectively. If $a = 0$ or $b = 0$, then both functions $\zeta(s;\mathfrak{a})$ and $\zeta(s,\alpha;\mathfrak{b})$ are entire. Clearly, $\zeta(s;\mathfrak{a})$ is a generalization of the Riemann zeta-function, and $\zeta(s,\alpha;\mathfrak{b})$ generalizes the Hurwitz zeta-function.

In [3], a joint universality theorem on the approximation of a pair of analytic functions by shifts $\zeta(s+i\tau;\mathfrak{a})$ and $\zeta(s+i\tau,\alpha;\mathfrak{b})$ has been obtained. Let $D = \left\{s \in \mathbb{C} : \frac{1}{2} < \sigma < 1\right\}$. Denote by $\mathcal{K}$ the class of compact subsets of the strip D with connected complements, by $H(K)$, $K \in \mathcal{K}$, the class of continuous functions on K which are analytic in the interior of K, and by $H_0(K)$, $K \in \mathcal{K}$, the subclass of $H(K)$ of non-vanishing functions on K. We remind that a sequence of numbers a_n is multiplicative if $a_1 = 1$ and $a_{mn} = a_m a_n$ for all coprime integers m, n. Now we state the main result of [3].

Theorem 1.1 *Suppose that the sequence $\mathfrak{a}$ is multiplicative, and that the number α is transcendental. Let $K_1, K_2 \in \mathcal{K}$, $f_1(s) \in H_0(K_1)$, and $f_2(s) \in H(K_2)$. Then, for every $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \frac{1}{T} meas \left\{ \tau \in [0,T] : \sup_{s\in K_1} |\zeta(s+i\tau;\mathfrak{a}) - f_1(s)| < \varepsilon, \right.$$

$$\left. \sup_{s\in K_2} |\zeta(s+i\tau,\alpha;\mathfrak{b}) - f_2(s)| < \varepsilon \right\} > 0.$$

Here meas$A$ denotes the Lebesgue measure of a measurable set $A \subset \mathbb{R}$. Theorem 1.1 is a generalization of the Mishou theorem proved in [9] for the Riemann zeta and Hurwitz zeta-functions. Theorem 1.1 is the so-called continuous universality theorem because analytic functions are approximated by the continuous shifts $\zeta(s + i\tau; \mathfrak{a})$ and $\zeta(s + i\tau, \alpha; \mathfrak{b})$, $\tau \in \mathbb{R}$. The aim of this paper is to prove a discrete version of Theorem 1.1 where analytic functions are approximated by discrete shifts $\zeta(s + ikh; \mathfrak{a})$ and $\zeta(s + ikh, \alpha; \mathfrak{b})$, or, more generally, by shifts $\zeta(s + ikh_1; \mathfrak{a})$ and $\zeta(s + ikh_2, \alpha; \mathfrak{b})$, $k \in \mathbb{N}_0$, with fixed positive numbers h, h_1, and h_2.

Denote by $\mathcal{P}$ the set of all prime numbers, and define the set

$$L(\mathcal{P}, \alpha, h, \pi) = \left\{(\log p : \ p \in \mathcal{P}), (\log(m + \alpha) : \ m \in \mathbb{N}_0), \frac{\pi}{h}\right\}.$$

Theorem 1.2 *Suppose that the set $L(\mathcal{P}, \alpha, h, \pi)$ is linearly independent over the field of rational numbers $\mathbb{Q}$, and that the sequence $\mathfrak{a}$ is multiplicative. Let $K_1, K_2 \in \mathcal{K}$, $f_1(s) \in H_0(K_1)$, and $f_2(s) \in H(K_2)$. Then, for every $\varepsilon > 0$,*

$$\liminf_{N\to\infty} \frac{1}{N+1} \# \left\{0 \le k \le N : \ \sup_{s\in K_1} |\zeta(s + ikh; \mathfrak{a}) - f_1(s)| < \varepsilon, \right.$$

$$\left. \sup_{s\in K_2} |\zeta(s + ikh, \alpha; \mathfrak{b}) - f_2(s)| < \varepsilon \right\} > 0.$$

Now let

$$L(\mathcal{P}, \alpha, h_1, h_2, \pi) = \{(h_1 \log p : \ p \in \mathcal{P}), (h_2 \log(m + \alpha) : \ m \in \mathbb{N}_0), \pi\}.$$

We note that this set consists of all elements of two sequences in addition with the number π. Then we have the following generalization of Theorem 1.2:

Theorem 1.3 *Suppose that the set $L(\mathcal{P}, \alpha, h_1, h_2, \pi)$ is linearly independent over $\mathbb{Q}$, and that the sequence $\mathfrak{a}$ is multiplicative. Let $K_1, K_2 \in \mathcal{K}$, $f_1(s) \in H_0(K_1)$, and $f_2(s) \in H(K_2)$. Then, for every $\varepsilon > 0$,*

$$\liminf_{N\to\infty} \frac{1}{N+1} \# \left\{0 \le k \le N : \ \sup_{s\in K_1} |\zeta(s + ikh_1; \mathfrak{a}) - f_1(s)| < \varepsilon, \right.$$

$$\left. \sup_{s\in K_2} |\zeta(s + ikh_2, \alpha; \mathfrak{b}) - f_2(s)| < \varepsilon \right\} > 0.$$

Obviously, for $h_1 = h_2 = h$ Theorem 1.3 reduces to Theorem 1.2.

By the Nesterenko theorem [11], the numbers π and e^{π} are algebraically independent over $\mathbb{Q}$. Therefore, the set $L(\mathcal{P}, \alpha, h_1, h_2, \pi)$ with $\alpha = \pi^{-1}$ and rational h_1, h_2 is linearly independent over $\mathbb{Q}$.

Professor Wolfgang Schwarz was a mathematician with a broad outlook. Among other problems of probabilistic and analytic number theory, he was also interested in universality of zeta-functions, and this is confirmed by the paper [7].

2 Two Lemmas

For the proof of Theorem 1.3, we will apply the probabilistic approach based on a limit theorem on weakly convergent probability measures in the space of analytic functions. In this section, we present two lemmas which play an important role in the proof of such a limit theorem.

Let $\gamma = \{s \in \mathbb{C} : |s| = 1\}$, and

$$\Omega_1 = \prod_{p \in \mathcal{P}} \gamma_p \quad \text{and} \quad \Omega_2 = \prod_{m \in \mathbb{N}_0} \gamma_m,$$

where γ_p for all $p \in \mathcal{P}$ and $\gamma_m = \gamma$ for all $m \in \mathbb{N}_0$. By the classical Tikhonov theorem, with the product topology and pointwise multiplication, the tori Ω_1 and Ω_2 are compact topological abelian groups. Therefore, denoting by $\mathcal{B}(X)$ the Borel σ-field of the space X, we observe that on $(\Omega_j, \mathcal{B}(\Omega_j))$ the probability Haar measure m_{jH} can be defined, $j = 1, 2$. Denote by $\omega_1(p)$ the projection of $\omega_1 \in \Omega_1$ to the coordinate space γ_p, $p \in \mathcal{P}$, and by $\omega_2(m)$ the projection of $\omega_2 \in \Omega_2$ to the coordinate space γ_m, $m \in \mathbb{N}_0$. Then $\omega_1(p)$, $p \in \mathcal{P}$, and $\omega_2(m)$, $m \in \mathbb{N}_0$, are complex-valued random variables defined on the spaces $(\Omega_1, \mathcal{B}(\Omega_1), m_{1H})$ and $(\Omega_2, \mathcal{B}(\Omega_2), m_{2H})$, respectively.

We define one more set by $\Omega = \Omega_1 \times \Omega_2$. Then Ω is also a compact topological abelian group. This leads to the probability space $(\Omega, \mathcal{B}(\Omega), m_H)$ with the probability Haar measure m_H. We denote by $\omega = (\omega_1, \omega_2)$ the elements of Ω, where $\omega_j \in \Omega_j$, $j = 1, 2$..

Next, for $A \in \mathcal{B}(\Omega)$, let

$$Q_N(A) \stackrel{def}{=} \frac{1}{N+1} \#\left\{0 \le k \le N : \left((p^{-ikh_1} : p \in \mathcal{P}),\right.\right.$$
$$\left.\left.((m+\alpha)^{-ikh_2} : m \in \mathbb{N}_0)\right) \in A\right\}.$$

Lemma 2.1 *Suppose that the set $L(\mathcal{P}, \alpha, h_1, h_2, \pi)$ is linearly independent over $\mathbb{Q}$. Then Q_N converges weakly to the Haar measure m_H as $N \to \infty$.*

Proof We apply the Fourier transform method, and use similar arguments as in the proof of Lemma 7 in [3]; recalling the proof of this lemma, we observe that the Fourier transform $g_N(\underline{k}, \underline{l})$, $\underline{k} = (k_p : k_p \in \mathbb{Z}, p \in \mathcal{P})$, $\underline{l} = (l_m : l_m \in \mathbb{Z}, m \in \mathbb{N}_0)$ of the measure Q_N is of the form

$$g_N(\underline{k}, \underline{l}) = \int_{\Omega} \left(\prod_{p \in \mathcal{P}} \omega_1^{k_p}(p) \prod_{m \in \mathbb{N}_0} \omega_2^{k_m}(m) \right) \mathrm{d}Q_N,$$

where only a finite number of integers k_p and l_m are distinct from zero. Thus, by the definition of Q_N,

$$g_N(\underline{k},\underline{l}) = \frac{1}{N+1}\sum_{k=0}^{N}\prod_{p\in\mathcal{P}} p^{-ikk_ph_1}\prod_{m\in\mathbb{N}_0}(m+\alpha)^{-ikl_mh_2}$$

$$= \frac{1}{N+1}\sum_{k=0}^{N}\exp\left\{-ikh_1\sum_{p\in\mathcal{P}}k_p\log p - ikh_2\sum_{m\in\mathbb{N}_0}l_m\log(m+\alpha)\right\}, \tag{2.1}$$

where, as above, only a finite number of integers k_p and l_m are distinct from zero. Obviously,

$$g_N(\underline{0},\underline{0}) = 1. \tag{2.2}$$

Before to consider the case $(\underline{k},\underline{l}) \neq (\underline{0},\underline{0})$, we observe that, in this case,

$$\exp\left\{-ih_1\sum_{p\in\mathcal{P}}k_p\log p - ih_2\sum_{m\in\mathbb{N}_0}l_m\log(m+\alpha)\right\} \neq 1. \tag{2.3}$$

Indeed, if inequality (2.3) is not true, then, for a certain $\hat{m}\in\mathbb{Z}$,

$$\exp\left\{-ih_1\sum_{p\in\mathcal{P}}k_p\log p - ih_2\sum_{m\in\mathbb{N}_0}l_m\log(m+\alpha)\right\} = e^{2\pi i\hat{m}}.$$

Hence,

$$h_1\sum_{p\in\mathcal{P}}k_p\log p + h_2\sum_{m\in\mathbb{N}_0}l_m\log(m+\alpha) = \pi\hat{l}$$

with $\hat{l}\in\mathbb{Z}$. Since only a finite number of integers k_p and l_m are distinct from zero, this contradicts the linear independence of the set $L(\mathcal{P},\alpha,h_1,h_2,\pi)$. Thus, (2.3) is true. Therefore, in the case $(\underline{k},\underline{l}) \neq (\underline{0},\underline{0})$, using the formula for the geometric series, we obtain

$$g_N(\underline{k},\underline{l}) = \frac{1-\exp\left\{-i(N+1)\left(h_1\sum\limits_{p\in\mathcal{P}}k_p\log p+h_2\sum\limits_{m\in\mathbb{N}_0}l_m\log(m+\alpha)\right)\right\}}{(N+1)\left(1-\exp\left\{-i\left(h_1\sum\limits_{p\in\mathcal{P}}k_p\log p+h_2\sum\limits_{m\in\mathbb{N}_0}l_m\log(m+\alpha)\right)\right\}\right)}.$$

From this and (2.2), we find that

$$\lim_{N\to\infty} g_N(\underline{k},\underline{l}) = \begin{cases} 1 & \text{if} \quad (\underline{k},\underline{l}) = (\underline{0},\underline{0}), \\ 0 & \text{if} \quad (\underline{k},\underline{l}) \neq (\underline{0},\underline{0}). \end{cases}$$

Therefore, a continuity theorem for probability measures on compact groups proves the lemma.

The next lemma uses again the linear independence of the set $L(\mathcal{P},\alpha,h_1,h_2,\pi)$ over $\mathbb{Q}$, and is devoted to ergodicity of a certain transformation on the space $(\Omega,\mathcal{B}(\Omega),m_H)$.

Define the element $a_{\alpha,h_1,h_2} \in \Omega$ by the formula

$$a_{\alpha,h_1,h_2} = \left\{(p^{-ih_1} : p \in \mathcal{P}), ((m+\alpha)^{-ih_2} : m \in \mathbb{N}_0)\right\},$$

and let, for $\omega \in \Omega$,

$$\varphi_{\alpha,h_1,h_2}(\omega) = a_{\alpha,h_1,h_2}\omega.$$

Since the Haar measure m_H is invariant with respect to translations by points from Ω, we have that φ_{α,h_1,h_2} is a measurable measure preserving transformation on the probability space $(\Omega,\mathcal{B}(\Omega),m_H)$. We remind that a set $A \in \mathcal{B}(\Omega)$ is called invariant with respect to the transformation φ_{α,h_1,h_2} if the sets A and $\varphi_{\alpha,h_1,h_2}(A)$ differ one from another at most by a set of zero m_H-measure, and that the transformation φ_{α,h_1,h_2} is ergodic if the σ-field of invariant sets consists of sets with m_H-measure 0 or 1.

Lemma 2.2 *Suppose that the set $L(\mathcal{P},\alpha,h_1,h_2,\pi)$ is linearly independent over $\mathbb{Q}$. Then the transformation φ_{α,h_1,h_2} is ergodic.*

Proof We know (see the proof of Lemma 11 of [3]) that characters χ of the group Ω are of the form

$$\chi(\omega) = \prod_{p\in\mathcal{P}} \omega_1^{k_p}(p) \prod_{m\in\mathbb{N}_0} \omega_2^{l_m}(m),$$

where only a finite number of integers k_p and l_m are distinct from zero. If χ is non-trivial character of Ω, then, from this and inequality (2.3), it follows that, for $(\underline{k},\underline{l}) \neq (\underline{0},\underline{0})$,

$$\chi(a_{\alpha,h_1,h_2}) = \exp\left\{-ih_1\sum_{p\in\mathcal{P}} k_p \log p - ih_2 \sum_{m\in\mathbb{N}_0} l_m \log(m+\alpha)\right\} \neq 1. \tag{2.4}$$

Let A be an invariant set of the transformation φ_{α,h_1,h_2}. Denote by I_A the indicator function of A, and by $\hat{f}$ the Fourier transform of the function f. Then

$$\hat{I}_A(\chi) = \int_\Omega \chi(\omega) I_A(\omega) m_H(\mathrm{d}\omega) = \chi(a_{\alpha,h_1,h_2}) \hat{I}_A(\chi),$$

since the measure m_H is invariant, and, for almost all $\omega \in \Omega$,

$$I_A(a_{\alpha,h_1,h_2}\omega) = I_A(\omega).$$

This and (2.4) imply that

$$\hat{I}_A(\chi) = 0 \tag{2.5}$$

for every non-trivial character χ of Ω.

Now let χ_0 be the trivial character of Ω, i.e., $\chi_0(\omega) \equiv 1$. Suppose that $\hat{I}(\chi_0) = a$. Since

$$\int_\Omega \chi(\omega) m_H(\mathrm{d}\omega) = \begin{cases} 1 & \text{if} \quad \chi = \chi_0, \\ 0 & \text{if} \quad \chi \neq \chi_0, \end{cases}$$

we have in view of (2.5) that, for every character χ of the group Ω,

$$\hat{I}_A(\chi) = a \int_\Omega \chi(\omega) m_H(\mathrm{d}\omega) = a\hat{1}(\chi) = \hat{a}(\chi). \tag{2.6}$$

It is well known that the function $I_A(\omega)$ is uniquely determined by its Fourier transform $\hat{I}_A(\omega)$. Therefore, we have from (2.6) that $I_A(\omega) = a$ for almost all $\omega \in \Omega$. However, since $I_A(\omega)$ is the indicator of A, $a = 0$ or 1. Hence, $I_A(\omega) = 0$ for almost all $\omega \in \Omega$, or $I_A(\omega) = 1$ for almost all $\omega \in \Omega$. This shows that $m_H(A) = 0$ or $m_H(A) = 1$, i.e., the transformation φ_{α,h_1,h_2} is ergodic.

3 A Limit Theorem

Denote by $H(D)$ the space of functions which are analytic on D, equipped with the topology of uniform convergence on compacta, and, for $A \in \mathcal{B}(H^2(D))$, define

$$P_N(A) = \frac{1}{N+1} \# \left\{ 0 \le k \le N : \ \underline{\zeta}(s + ik\underline{h}, \alpha; \mathfrak{a}, \mathfrak{b}) \in A \right\},$$

where $\underline{h} = (h_1, h_2)$ and

$$\underline{\zeta}(s + ik\underline{h}, \alpha; \mathfrak{a}, \mathfrak{b}) = (\zeta(s + ikh_1; \mathfrak{a}), \zeta(s + ikh_2, \alpha; \mathfrak{b})).$$

Moreover, on the probability space $(\Omega, \mathcal{B}(\Omega), m_H)$, define the $H^2(D)$-valued random element $\underline{\zeta}(s, \alpha, \omega; \mathfrak{a}, \mathfrak{b})$ by the formula, see [3],

$$\underline{\zeta}(s, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) = (\zeta(s, \omega_1; \mathfrak{a}), \zeta(s, \alpha, \omega_2; \mathfrak{b})),$$

where

$$\zeta(s, \omega_1; \mathfrak{a}) = \sum_{m=1}^{\infty} \frac{a_m \omega_1(m)}{m^s}$$

with

$$\omega_1(m) = \prod_{\substack{p^r \mid m \\ p^{r+1} \nmid m}} \omega_1^r(p),$$

and

$$\zeta(s, \alpha, \omega_2; \mathfrak{b}) = \sum_{m=0}^{\infty} \frac{b_m \omega_2(m)}{(m+\alpha)^s}.$$

We note that the series for $\zeta(s, \omega_1; \mathfrak{a})$ and $\zeta(s, \alpha, \omega_2; \mathfrak{b})$ converge uniformly on compact subsets of the strip D for almost all $\omega_1 \in \Omega_1$ and $\omega_2 \in \Omega_2$, respectively, and thus they define $H(D)$-valued random elements on the probability spaces $(\Omega_1, \mathcal{B}(\Omega_1), m_{1H})$ and $(\Omega_2, \mathcal{B}(\Omega_2), m_{2H})$, respectively. Moreover, in view of multiplicativity of the sequence $\mathfrak{a}$, we have that for almost all $\omega_1 \in \Omega_1$ and $s \in D$,

$$\zeta(s, \omega_1; \mathfrak{a}) = \prod_{p \in \mathcal{P}} \left(1 + \sum_{k=1}^{\infty} \frac{a_{p^k} \omega_1^k(p)}{p^{ks}}\right).$$

Let $P_{\underline{\zeta}}$ be the distribution of random element $\underline{\zeta}(s, \alpha, \omega; \mathfrak{a}, \mathfrak{b})$, i.e., let $P_{\underline{\zeta}}$ be a probability measure given by

$$P_{\underline{\zeta}}(A) = m_H\left(\omega \in \Omega : \underline{\zeta}(s, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) \in A\right), \quad A \in \mathcal{B}(H^2(D)).$$

Now we are ready to state a limit theorem for P_N. Let

$$S = \{g \in H(D) : g(s) \neq 0 \text{ or } g(s) \equiv 0\}.$$

Theorem 3.1 *Suppose that the set $L(\mathcal{P}, \alpha, h_1, h_2, \pi)$ is linearly independent over $\mathbb{Q}$, and that the sequence $\mathfrak{a}$ is multiplicative. Then P_N converges weakly to $P_{\underline{\zeta}}$ as $N \to \infty$. Moreover, the support of $P_{\underline{\zeta}}$ is the set $S \times H(D)$.*

Proof The proof is similar to the one for Theorem 6 from [3], therefore, we do not give all details.

For fixed $\sigma_1 > \frac{1}{2}$ and $m, n \in \mathbb{N}$, let

$$v(m,n) = \exp\left\{-\left(\frac{m}{n}\right)^{\sigma_1}\right\},$$

and for $m \in \mathbb{N}_0$, $n \in \mathbb{N}$,

$$v(m,n,\alpha) = \exp\left\{-\left(\frac{m+\alpha}{n+\alpha}\right)^{\sigma_1}\right\}.$$

Define the functions

$$\zeta_n(s;\mathfrak{a}) = \sum_{m=1}^{\infty} \frac{a_m v(m,n)}{m^s}$$

and

$$\zeta_n(s,\alpha;\mathfrak{b}) = \sum_{m=0}^{\infty} \frac{b_m v(m,n,\alpha)}{(m+\alpha)^s}.$$

Then it is known (see [2, 6]) that the latter series are absolutely convergent for $\sigma > \frac{1}{2}$. For brevity, let

$$\underline{\zeta}_n(s+ik\underline{h},\alpha;\mathfrak{a},\mathfrak{b}) = (\zeta_n(s+ikh_1;\mathfrak{a}), \zeta_n(s+ikh_2,\alpha;\mathfrak{b}))$$

and

$$P_{N,n}(A) = \frac{1}{N+1}\#\left\{0 \le k \le N : \ \underline{\zeta}_n(s+ik\underline{h},\alpha;\mathfrak{a},\mathfrak{b}) \in A\right\},$$
$$A \in \mathcal{B}(H^2(D)).$$

Similarly, for $\omega = (\omega_1, \omega_2) \in \Omega$, define

$$\zeta_n(s,\omega_1;\mathfrak{a}) = \sum_{m=1}^{\infty} \frac{a_m \omega_1(m) v(m,n)}{m^s}$$

and

$$\zeta_n(s,\alpha,\omega_2;\mathfrak{b}) = \sum_{m=0}^{\infty} \frac{b_m \omega_2(m) v(m,n,\alpha)}{(m+\alpha)^s},$$

the series also being absolutely convergent for $\sigma > \frac{1}{2}$. Let

$$\underline{\zeta}_n(s + ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) = (\zeta_n(s + ikh_1, \omega_1; \mathfrak{a}), \zeta_n(s + ikh_2, \alpha, \omega_2; \mathfrak{b})),$$

and

$$P_{N,n,\omega}(A) = \frac{1}{N+1}\#\left\{0 \le k \le N : \ \underline{\zeta}_n(s + ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) \in A\right\},$$

$$A \in \mathcal{B}(H^2(D)).$$

Now, using Lemma 2.1, Theorem 5.1 of [1] and the invariance of the Haar measure m_H, we easily find that, on $(H^2(D), \mathcal{B}(H^2(D)))$, there exists a probability measure P_n such that the measures $P_{N,n}$ and $P_{N,n,\omega}$ both converge weakly to P_n as $N \to \infty$. The latter assertion is an analogue of Theorem 8 from [3].

The next step of the proof of Theorem 3.1 consists of approximation. For this purpose, the metric of $H^2(D)$ is substantial. It is well known that there exists a sequence of compact sets $\{K_l : \ l \in \mathbb{N}\} \subset D$ such that

$$D = \bigcup_{l=1}^{\infty} K_l,$$

$K_l \subset K_{l+1}$ for $l \in \mathbb{N}$, and if $K \subset D$ is a compact set, then $K \subset K_l$ for some l. For $g_1, g_2 \in H(D)$, define

$$\rho(g_1, g_2) = \sum_{l=1}^{\infty} 2^{-l} \frac{\sup_{s \in K_l} |g_1(s) - g_2(s)|}{1 + \sup_{s \in K_l} |g_1(s) - g_2(s)|}.$$

Then ρ is a metric on $H(D)$ which induces the topology of uniform convergence on compacta. Now if, for $\underline{g}_1 = (g_{11}, g_{12})$, $\underline{g}_2 = (g_{21}, g_{22}) \in H^2(D)$,

$$\underline{\rho}(\underline{g}_1, \underline{g}_2) = \max_{j=1,2} \rho(g_{1j}, g_{2j}),$$

then $\underline{\rho}$ is a metric in $H^2(D)$ inducing its topology.

We also remind the Gallagher lemma, Lemma 1.4 of [10], which allows to deduce discrete mean square estimates from those of continuous type.

Lemma 3.2 *Let T_0 and $T \ge \delta > 0$ be real numbers, and let $\mathcal{T}$ be a finite set lying in the interval $[T_0 + \frac{\delta}{2}, T_0 + T - \frac{\delta}{2}]$. Define*

$$N_\delta(x) = \sum_{\substack{t \in \mathcal{T} \\ |t-x| < \delta}} 1,$$

and let $S(x)$ be a complex-valued continuous function on $[T_0, T + T_0]$ having a continuous derivative on $(T_0, T + T_0)$. Then

$$\sum_{t\in\mathcal{T}} N_\delta^{-1}(t)|S(t)|^2 \le \frac{1}{\delta}\int_{T_0}^{T}|S(x)|^2dx + \left(\int_{T_0}^{T}|S(x)|^2dx\int_{T_0}^{T}|S'(x)|^2dx\right)^{\frac{1}{2}}.$$

For $n \in \mathbb{N}$, let

$$l_n(s) = \frac{s}{\sigma_1}\Gamma\left(\frac{s}{\sigma_1}\right)n^s,$$

where $\Gamma(s)$ is the Euler gamma-function. Then an application of the Mellin formula

$$\frac{1}{2\pi i}\int_{b-i\infty}^{b+i\infty}\Gamma(s)a^{-s}\mathrm{d}s = e^{-a}, \quad a,\ b > 0,$$

leads to the representation

$$\zeta_n(s;\mathfrak{a}) = \frac{1}{2\pi i}\int_{b-i\infty}^{b+i\infty}\zeta(s+z;\mathfrak{a})l_n(z)\frac{\mathrm{d}z}{z}.$$

Let $K \subset D$ be a compact subset. Then the above representation for $\zeta_n(s;\mathfrak{a})$ and an application of the residue theorem imply, for an arbitrary $h_1 > 0$, the estimate

$$\begin{aligned}&\frac{1}{N}\sum_{k=0}^{N}\sup_{s\in K}|\zeta(s+ikh_1;\mathfrak{a}) - \zeta_n(s+ikh_1;\mathfrak{a})|\\ &\ll \int_{-\infty}^{\infty}|l_n(\hat{\sigma}+i\tau)|\left(\frac{1}{N}\sum_{k=0}^{N}|\zeta(\sigma+it+ikh_1+i\tau;\mathfrak{a})|\right)\mathrm{d}t, \qquad (3.1)\end{aligned}$$

where $\hat{\sigma} < 0$, $\frac{1}{2} < \sigma < 1$ and t is bounded by a constant. Since, for a fixed σ, $\frac{1}{2} < \sigma < 1$, the estimate [6]

$$\int_0^T|\zeta(\sigma+it;\mathfrak{a})|^2\mathrm{d}t = O(T)$$

is valid, Lemma 3.2 implies the bound

$$\frac{1}{N}\sum_{k=0}^{N}|\zeta(\sigma+\boldsymbol{it}+ikh_1+i\tau;\mathfrak{a})| \le \left(\frac{1}{N}\sum_{k=0}^{N}|\zeta(\sigma+\boldsymbol{it}+ikh_1+i\tau;\mathfrak{a})|^2\right)^{\frac{1}{2}}$$

$$\le \frac{1}{h_1}\int_0^{Nh_1}|\zeta(\sigma+it+i\tau;\mathfrak{a})|^2dt+$$

$$\left(\int_0^{Nh_1}|\zeta(\sigma+it+i\tau;\mathfrak{a})|^2dt\int_0^{Nh_1}|\zeta'(\sigma+it+i\tau;\mathfrak{a})|^2dt\right)^{\frac{1}{2}} \ll 1+|\omega\tau|.$$

Therefore, in view of (3.1),

$$\lim_{n\to\infty}\limsup_{N\to\infty}\frac{1}{N+1}\sum_{k=0}^{N}\sup_{s\in K}|\zeta(s+ikh_1;\mathfrak{a})-\zeta_n(s+ikh_1;\mathfrak{a})| = 0.$$

From this, by the definition of the metric ρ, we find that

$$\lim_{n\to\infty}\limsup_{N\to\infty}\frac{1}{N+1}\sum_{k=0}^{N}\rho\left(\zeta(s+ikh_1;\mathfrak{a}),\zeta_n(s+ikh_1;\mathfrak{a})\right) = 0. \tag{3.2}$$

In [5], Theorem 4.1, it was shown that for an arbitrary $h_2 > 0$ and a compact subset $K \subset D$,

$$\lim_{n\to\infty}\limsup_{N\to\infty}\frac{1}{N+1}\sum_{k=0}^{N}\sup_{s\in K}|\zeta(s+ikh_2,\alpha;\mathfrak{b})-\zeta_n(s+ikh_2,\alpha;\mathfrak{b})| = 0.$$

Thus,

$$\lim_{n\to\infty}\limsup_{N\to\infty}\frac{1}{N+1}\sum_{k=0}^{N}\rho\left(\zeta(s+ikh_2,\alpha;\mathfrak{b}),\zeta_n(s+ikh_2,\alpha;\mathfrak{b})\right) = 0.$$

The latter equality together with (3.2) and the definition of the metric $\underline{\rho}$ shows that

$$\lim_{n\to\infty}\limsup_{N\to\infty}\frac{1}{N+1}\sum_{k=0}^{N}\underline{\rho}\left(\underline{\zeta}(s+ik\underline{h},\alpha;\mathfrak{a},\mathfrak{b}),\underline{\zeta}_n(s+ik\underline{h},\alpha;\mathfrak{a},\mathfrak{b})\right) = 0. \tag{3.3}$$

Standard arguments show that for almost all $\omega_1 \in \Omega_1$,

$$\int_0^T|\zeta(\sigma+it,\omega_1;\mathfrak{a})|^2\mathrm{d}t = O(T)$$

with a fixed σ, $\frac{1}{2} < \sigma < 1$. Therefore, by a reasoning as in the proof of (3.2) we find that, for almost all $\omega_1 \in \Omega_1$,

$$\lim_{n\to\infty} \limsup_{N\to\infty} \frac{1}{N+1} \sum_{k=0}^{N} \rho\left(\zeta(s+ikh_1, \omega_1; \mathfrak{a}), \zeta_n(s+ikh_1, \omega_1; \mathfrak{a})\right) = 0. \tag{3.4}$$

The linear independence over $\mathbb{Q}$ of the set $L(\mathcal{P}, \alpha, h_1, h_2, \pi)$ implies the linear independence of the set

$$\left\{ ((m+\alpha) : \ m \in \mathbb{N}_0), \frac{\pi}{h_2} \right\}.$$

Thus, repeating the proof of Lemma 2.6 of [4], we have that for almost all $\omega_2 \in \Omega_2$,

$$\lim_{n\to\infty} \limsup_{N\to\infty} \frac{1}{N+1} \sum_{k=0}^{N} \rho\left(\zeta(s+ikh_2, \alpha, \omega_2; \mathfrak{b}), \zeta_n(s+ikh_2, \alpha, \omega_2; \mathfrak{b})\right) = 0.$$

This together with (3.4), for almost all $\omega \in \Omega$, implies the equality

$$\lim_{n\to\infty} \limsup_{N\to\infty} \frac{1}{N+1} \sum_{k=0}^{N} \underline{\rho}\left(\underline{\zeta}(s+ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}), \underline{\zeta}_n(s+ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b})\right) = 0, \tag{3.5}$$

where

$$\underline{\zeta}(s+ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) = (\zeta(s+ikh_1, \omega_1; \mathfrak{a}), \zeta(s+ikh_2, \alpha, \omega_2; \mathfrak{b})).$$

For $\omega \in \Omega$, we define one more probability measure by

$$P_{N,\omega}(A) = \frac{1}{N+1} \# \left\{ 0 \le k \le N : \ \underline{\zeta}(s+ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) \in A \right\}, \quad A \in \mathcal{B}(H^2(D)).$$

Then the weak convergence of $P_{N,n}$ and $P_{N,n,\omega}$ to the same measure P_n as $N \to \infty$, equalities (3.3) and (3.5), and Theorem 4.2 of [1] show that the measures P_N and $P_{N,\omega}$ both converge weakly to the same probability measure P on $(H^2(D), \mathcal{B}(H^2(D)))$ as $N \to \infty$.

It remains to prove that $P = P_{\underline{\zeta}}$. For this, Lemma 2.2 is applied. On the space $(\Omega, \mathcal{B}(\Omega), m_H)$, define the random variable θ by the formula

$$\theta(\omega) = \begin{cases} 1 & \text{if} \quad \underline{\zeta}(s, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) \in A, \\ 0 & \text{otherwise}, \end{cases}$$

where A is a fixed continuity set of the measure P. Then, for the expectation $\mathbb{E}\theta$, we have

$$\mathbb{E}\theta = \int_{\Omega} \theta \mathrm{d}m_H = P_{\underline{\zeta}}(A). \tag{3.6}$$

Lemma 2.2 together with the Birkhoff–Khintchine ergodicity theorem yields the equality

$$\lim_{N\to\infty} \frac{1}{N+1} \sum_{k=0}^{N} \theta\left(\varphi^k_{\alpha,h_1,h_2}(\omega)\right) = \mathbb{E}\theta. \tag{3.7}$$

On the other hand, by the definitions of θ and φ_{α,h_1,h_2}, we have that

$$\frac{1}{N+1} \sum_{k=0}^{N} \theta\left(\varphi^k_{\alpha,h_1,h_2}(\omega)\right) = P_{N,\omega}(A). \tag{3.8}$$

Since $P_{N,\omega}$ converges weakly to P, and A is a continuity set of P, it follows that

$$\lim_{N\to\infty} P_{N,\omega}(A) = P(A).$$

However, (3.6)–(3.8) imply that, for every continuity set A of P,

$$P_{\underline{\zeta}}(A) = P(A).$$

Hence, $P_{\underline{\zeta}} = P$.

The limit measure $P_{\underline{\zeta}}$ does neither depend on h_1 and h_2 nor on the arithmetic of α. Therefore, by Lemma 12 of [3], the support of $P_{\underline{\zeta}}$ is the set $S \times H(D)$. The theorem is proved.

4 Proof of the Universality Theorem

A proof of Theorem 1.3 is based on Theorem 3.1 and the Mergelyan theorem on the approximation of analytic functions by polynomials, and is quite standard. We state the Mergelyan theorem as the following lemma:

Lemma 4.1 *Let $K \subset \mathbb{C}$ be a compact set with connected complement, and let $f(s)$ be a continuous function on K which is analytic in the interior of K. Then, for every $\varepsilon > 0$, there exists a polynomial $p(s)$ such that*

$$\sup_{s\in K} |f(s) - p(s)| < \varepsilon.$$

The proof of this lemma can be found in [8] and [12].

We will also use an equivalent of the weak convergence of probability measures in terms of open sets.

Lemma 4.2 *Suppose that P_n, $n \in \mathbb{N}$, and P are probability measures on $(X, \mathcal{B}(X))$. Then P_n converges weakly to P as $n \to \infty$ if, and only if, for every open set $G \subset X$,*

$$\liminf_{n\to\infty} P_n(G) \geq P(G).$$

The proof of this lemma is given in [1], Theorem 2.1.

Proof (Proof of Theorem 1.3) By Lemma 4.2, there exist polynomials $p_1(s)$ and $p_2(s)$ such that

$$\sup_{s\in K_1} \left|f_1(s) - e^{p_1(s)}\right| < \frac{\varepsilon}{2}. \tag{4.1}$$

and

$$\sup_{s\in K_2} |f_2(s) - p_2(s)| < \frac{\varepsilon}{2}. \tag{4.2}$$

Define the set

$$G = \left\{(g_1, g_2) \in H^2(D) : \sup_{s\in K_1} \left|g_1(s) - e^{p_1(s)}\right| < \frac{\varepsilon}{2}, \sup_{s\in K_2} |g_2(s) - p_2(s)| < \frac{\varepsilon}{2}\right\}.$$

Then we observe that G is an open set, and, in view of the second assertion of Theorem 3.1, $(e^{p_1(s)}, p_2(s))$ is an element of the support of the measure $P_{\underline{\zeta}}$. Therefore, $P_{\underline{\zeta}}(G) > 0$. Thus, by first assertion of Theorem 3.1 and Lemma 4.2,

$$\liminf_{N\to\infty} \frac{1}{N+1} \#\left\{0 \leq k \leq N : \underline{\zeta}(s + ik\underline{h}, \alpha, \omega; \mathfrak{a}, \mathfrak{b}) \in G\right\} \geq P_{\underline{\zeta}}(G) > 0.$$

Therefore, the definition of G implies that

$$\liminf_{N\to\infty} \frac{1}{N+1} \#\left\{0 \leq k \leq N : \sup_{s\in K_1} \left|\zeta(s + ikh_1; \mathfrak{a}) - e^{p_1(s)}\right| < \frac{\varepsilon}{2},\right.$$

$$\left.\sup_{s\in K_2} |\zeta(s + ikh_2, \alpha; \mathfrak{b}) - p_2(s)| < \frac{\varepsilon}{2}\right\} > 0.$$

Combining this with (4.1) and (4.2) proves the theorem.

References

1. P. Billingsley, *Convergence of Probability Measures* (Wiley, New York, 1968)
2. A. Javtokas, A. Laurinčikas, On the periodic Hurwitz zeta-function. Hardy-Ramanujan J. **29**, 18–36 (2006)
3. R. Kačinskaitė, A. Laurinčikas, The joint distribution of periodic zeta-functions. Studia Sci. Math. Hung. **48**(2), 257–279 (2011)
4. A. Laurinčikas, A discrete universality theorem for the Hurwitz zeta-function. J. Number Theory **143**, 232–247 (2014)
5. A. Laurinčikas, R. Macaitienė, The discrete universality of the periodic Hurwitz zeta-function. Integral Transf. Spec. Funct. **20**(9–10), 673–686 (2009)
6. A. Laurinčikas, D. Šiaučiūnas, Remarks on the universality of periodic zeta-functions. Mat. Zametki **80**(4), 561–568 (2006) (in Russian); Math. Notes **80**(3–4), 532–538 (2006)
7. A. Laurinčikas, W. Schwarz, J. Steuding, The universality of general Dirichlet series. Analysis **23**, 13–26 (2003)
8. S.N. Mergelyan, Uniform approximations to functions of a complex variable. Uspekhi Matem. Nauk **7**(2), 31–122 (1952) (in Russian); American Mathematical Society Translations. Ser. 1, vol. 3, Series and Approximation (American Mathematical Society, Providence, 1969), pp. 294–391
9. H. Mishou, The joint value distribution of the Riemann zeta-function and Hurwitz zeta-functions. Lith. Math. J. **47**(1), 32–47 (2007)
10. H.L. Montgomery, *Topics in Multiplicative Number Theory*. Lecture Notes in Mathematics, vol. 227 (Springer, Berlin, 1971)
11. Yu.V. Nesterenko, Modular functions and transcendence questions. Mat. Sb. **187**(9), 65–96 (1996) (in Russian); Sb. Math. **187**(9), 1319–1348 (1996)
12. J.L. Walsh, *Interpolation and Approximation by Rational Functions in the Complex Domain*. American Mathematical Society Colloquium Publications, vol. 20 (American Mathematical Society, Providence, 1960)

Remembering Wolfgang Schwarz, His Life and Work

Lutz G. Lucht

Abstract The essay is the author's very personal retrospective on the life and work of Wolfgang Schwarz. Besides biographical details of Schwarz's private life and his professional career, it gives account of his work on multiplicative functions in collaboration with several colleagues.

Keywords Multiplicative functions • Wolfgang Schwarz

2010 Mathematics subject classification: Primary 01A70; Secondary 11M41

On July 19, 2013, Wolfgang Schwarz passed away in his home in Kelkheim after a serious disease. He was an outstanding, highly prolific, scientifically influential and innovative number theorist of international renown, a good friend, and a masterful teacher. His far-ranging professional work in pure mathematics was devoted to the large family of mathematics students and researchers. In his papers, monographs, lectures, and talks, he liked to share ideas and discoveries in mathematics with experts as well as with a broad audience. His passing is a severe loss to the field of mathematics in general, and to the theory of arithmetic functions in particular, and his loss will be deeply felt.

Wolfgang is survived by his wife Doris and daughters Karin and Eva with their families including six grandchildren, to whom he was a devoted husband, father, and grandfather. He and Doris were married for more than five decades and endured some tremendous hardships, but never lost their courage to face life. BothWolfgang and his wife, who quickly became a real actor in the mathematical world, supported numerous mathematicians by invitations, great hospitality, and warmth in their home in Kelkheim. Those of us who were their guests will treasure these happy memories.

L.G. Lucht (✉)
Siemensstr. 1, 38640 Goslar, Germany
e-mail: m.lg@online.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_16

Published with kind permission of © Doris Schwarz, 2013

1 Early Years

Wolfgang Schwarz was born on April 21, 1934, in Selb, a small town located in the Fichtel mountains, famous for the Rosenthal porcelain manufacturer, at the North-East of Bavaria near the borders to Thuringia and Saxony. There he developed a sportive passion for hiking, mountaineering, and skiing already in young years.

At age 10, he lost his father in WW II, a bitter fate that he shared with many children during those war times. Due to his talents, diligence, versatility, and sportsmanship Schwarz mastered the Gymnasium with excellence during the difficult postwar period. He obtained the Abitur at age 17. In addition to his sporting activities he emerged as a very good chess and piano player.

Supported by a Hundshammer scholarship he studied mathematics and physics for a teaching certificate at the University of Erlangen-Nürnberg from 1951 until 1956. His thesis on transcendental p-adic numbers was supervised by Theodor Schneider. Schneider, a student of Carl Ludwig Siegel, is well known for his solution of the 7th Hilbert problem—independently from Gelfond—in his 1934 Frankfurt dissertation.

Until 1960 Schwarz was Schneider's assistant and obtained his doctorate in 1959 with a dissertation on additive prime power representations of positive integers. His subsequent time at the university of Freiburg certainly was the happiest period in Wolfgang Schwarz's life, as he enjoyed the loyal atmosphere and high standards of the department, and the good libraries in Freiburg and the nearby Oberwolfach; he made life-long friends and, in particular, he met his wife Doris.

Although mathematics took most of his time, he kept up a multitude of activities such as playing chess on a high level, mountaineering, and climbing, even when he was short on time. This is shown by the photos (Figs. 1 and 2).

Fig. 1 Bavarian Chess Congress, Bad Kissingen, 1954. Published with kind permission of © Doris Schwarz, 2013

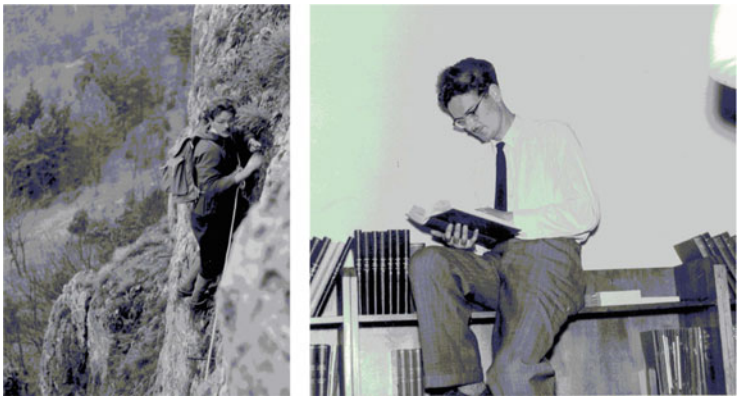


Fig. 2 On the *left*: mountaineering, ≈1955; on the *right*: climbing in the Freiburg Library, ≈1960. Published with kind permission of © Doris Schwarz, 2013

2 Survey of Schwarz's Career and Work

When Schneider was appointed to a full professorship at the University of Freiburg in 1960, he took Schwarz as postdoctoral research fellow with him to Freiburg. There Schwarz obtained the habilitation in 1964 with a thesis on Tauberian theorems, received a position as lecturer and, in 1969, as professor.

In the same year he was appointed to a full professorship at the University of Frankfurt/Main, where he reestablished an internationally respected number theory research group.

The impressive list of Wolfgang Schwarz's scientific ancestors dates back to the early eighteenth century and contains some of the most famous mathematicians of the modern age:

Christian August Hansen		
Abraham Gotthelf Köstner	1739	Leipzig
Johann Friedrich Pfaff	1788	Helmstedt
Carl Friedrich Gauß	1799	Helmstedt
Christoph Gudermann	1841	Göttingen
Karl Theodor Wilhelm Weierstraß	1854	Königsberg
Georg Ferdinand Frobenius	1870	Berlin
Edmund Landau	1899	Berlin
Carl Ludwig Siegel	1920	Göttingen
Theodor Schneider	1934	Frankfurt am Main
Wolfgang Karl Schwarz	1959	Erlangen-Nürnberg

In Wolfgang Schwarz's early years, sieve methods, Tauberian theorems, and the boundary behavior of power series dominated his research. Later he focused on Banach algebras, multiplicative semigroups, and inversion of arithmetic functions, the approximation of arithmetic functions by exponential functions, structural properties of algebras of almost-even arithmetic functions, their mean behavior and Fourier-Ramanujan expansions, classes of non-multiplicative, non-additive, iterated or shifted arithmetic functions and their properties.

He published more than 120 papers and monographs and was a very successful academic teacher guiding fourteen doctoral students. The topics of their dissertations reflect the breadth of his mathematical interests.

Karl-Heinz Indlekofer	1970	Freiburg
Johannes Duttlinger	1972	Frankfurt
Ernst Heppner	1974	Frankfurt
Evelyn Brinitzer	1977	Frankfurt
Manfred Gottschalk	1977	Frankfurt
Bruno Tenderra	1977	Frankfurt
Thomas Maxsein	1985	Frankfurt
Joachim Herzog	1987	Frankfurt
Peter Kunth	1988	Frankfurt
Kurt Höhne	1991	Frankfurt
Rainer Tschiersch	1995	Frankfurt
Peter Bauer	1997	Frankfurt
Christian Elsholtz	1998	Darmstadt
Matthias Frost	2008	Frankfurt

Supported by Wolfgang Schwarz, Karl-Heinz Indlekofer, Bohuslav Divič, Ernst Heppner, and Jörn Steuding obtained their habilitation at Frankfurt University.

Three of them, Karl-Heinz Indlekofer in Paderborn, Jörn Steuding in Würzburg and Christian Elsholtz in Graz, have followed in his footsteps as university teachers and researchers. Numerous students, assistants, and colleagues were fascinated by his courses, lectures, papers, and monographs, his versatile insight, his generous helpfulness, and his interest in imparting his rich knowledge. They were stimulated to enhance his methods and results and to contribute to the solution of resulting mathematical problems, and will always remember him with gratitude.

Wolfgang Schwarz's monographs on prime number theory [20], sieve methods [25], elementary number theory [26], and arithmetical functions [32], the latter jointly written with Jürgen Spilker (Freiburg), resulted from his research interests and preparations of courses given in Freiburg and Frankfurt. They contain a large number of footnotes with valuable hints and thoroughly researched bibliographical remarks, a specialty of Schwarz's publications. In particular, the monograph *Arithmetical Functions* has established itself as standard reference in this area of number theory, to which both the authors and their students have contributed many significant results.

In the recent past Wolfgang Schwarz was also engaged in research in the history of mathematics. An important aspect was the Mathematical Seminar of Frankfurt University, the fate of mathematicians in Frankfurt after 1930 (see the remarkable Festschrift [30]), and the history of number theory (Fig. 3).

In addition to many official duties in Frankfurt, Wolfgang Schwarz was active as

- Longtime member of the *Mathematical Seminar of Frankfurt University*
- Longtime member of the *Wissenschaftliche Gesellschaft* at Frankfurt University
- Longtime trustee of the Catholic Church's *Cusanuswerk* at Frankfurt University
- Co-organizer (with H.-E. Richert and E. Wirsing) of the MFI Oberwolfach conferences on *Elementary and Analytical Number Theory* from 1974 to 1994
- President of the *Deutsche Mathematiker-Vereinigung* from 1986 to 1987

Fig. 3 Inaugural address at the Annual Convention of the DMV, Berlin, 1987. Published with kind permission of © Doris Schwarz, 2013

- Longtime member of the *DMV* executive board
- Spokesperson of the *Konferenz der Mathematischen Fachbereiche* from 1992 to 1993
- Organizer of the 3rd *ELAZ-Conference* in Mainz and the preceding *Number Theory Day* in Frankfurt in 2004
- Author, editor, and translator of more than 120 research papers and several books
- Co-editor (with P.T. Bateman, L. Mirsky, H.L. Montgomery, W. Schaal, I.J. Schoenberg, H. Wefelscheid) of Edmund Landau's *Collected Works* in nine volumes, 1985–1987
- External supervisor and reviewer of numerous doctoral and habilitation theses, and papers

Wolfgang Schwarz mastered a tremendous workload which he sometimes put on hold in favor of his family, of recreation, of joint ventures with friends, or simply of leisure activities (Figs. 4 and 5).

Sometimes joint ventures with friends also consisted of walks in the hills depending on adequate weather. Unseasonal conditions could then lead to a joint mathematical paper. For instance, the first footnote in a joint paper with Spilker [31] from 1983 might have originated in bad weather during a joint hiking tour in Austria. (It says: *The draft of this note resulted from joint mountain hikes in Rätikon and in Ötztal*.) In 1982, I received a copy of the preprint which I picked from my collection of Schwarz's papers:

EINE BEMERKUNG ZUR CHARAKTERISIERUNG DER FAST-PERIODISCHEN MULTIPLIKATIVEN ZAHLENTHEORETISCHEN FUNKTIONEN MIT VON NULL VERSCHIEDENEM MITTELWERT[1)]

Wolfgang Schwarz
Jürgen Spilker

ABSTRACT.

Denote by $\mathscr{A}^q$ the vector space of B^q-almost-periodic arithmetical functions. H. Daboussi [2], [3] and P.D.T.A. Elliott [8], [10] characterized the set of multiplicative functions in $\mathscr{A}^q$ with mean-value $M(f) \neq 0$ by a statement concerning the convergence of certain series extended over the values $f(p^k)$ of f at prime powers (see (1.2_1), (1.2_2), and (1.2_3)). The authors give a simpler proof for the implication: If $f \in \mathscr{A}^q$ $(q \geq 1)$ is multiplicative with mean-value $M(f) \neq 0$, then the series mentioned above are convergent. The proof consists in reducing the assertion to the special case $q = 2$, for which a simple proof is available by Daboussi - Delange [3] (see also [24]).

AMS classification: 10H45, 10K35.

[1)] Im Entwurf entstand diese Note auf gemeinsamen Bergtouren im Rätikon und im Ötztal.

Fig. 4 Making music with Peter Elliott, Oberwolfach, ≈1994. Published with kind permission of © Doris Schwarz, 2013

Fig. 5 Skiing in front of the Königsspitze in Sulden, South Tirol, ≈1996. Published with kind permission of © Doris Schwarz, 2013

Despite receiving notable enquiries from other universities, Wolfgang Schwarz remained in Frankfurt. After becoming an emeritus in 2002, he continued research, published papers, attended conferences, gave lectures, and supported many young academics until 2012.

3 Reminiscences

I met Wolfgang Schwarz for the first time in the winter semester 1970/71. He was invited to give a colloquium talk in Clausthal which focused on the algebra of arithmetic functions and the subgroup of multiplicative functions under the Dirichlet convolution together with many applications, a topic that influenced my later teaching and research.

In the same semester Eduard Wirsing was also invited, and I could easily guess that both had been chosen by the faculty as external reviewers of my impending habilitation with a thesis on the asymptotic behavior of sums of multiplicative functions, closing a gap between results of Wirsing and those of Schwarz.

A few days after Schwarz's talk, I received a small parcel with offprints. This turned into a regular correspondence and the exchange of preprints of many papers, and I was frequently invited to attend the Oberwolfach conferences on Elementary and Analytic Number Theory.

When I was asked to give a seminar talk at Frankfurt University in June, 1974, Schwarz had reserved the department's guest room in the mathematics tower building. After my arrival and a brief check-in he took me to his and his family's newly built Taunus home where Mrs. Schwarz prepared a dinner for all members and guests of his institute. The evening with about 12 persons was a stunning event, not only because of the excellent dinner (in particular, I remember the homemade Frankfurt Green Sauce, a local specialty), but also because of the hospitality and warmth, combined with good conversation and human attention. I immediately realized the sharp contrast to the atmosphere of the ugly tower building and its dirty surroundings. Let me recall that during the second half of the 1970s, Frankfurt was marked by fierce student's protests, the APO (a radical student organization), and the emerging terrorist RAF.

A few weeks after my Frankfurt talk I obtained a letter from Wolfgang Schwarz which contained a draft of an extension of the result presented in my talk; this led to a joint paper [18]. From the late 1980s on the correspondence was eased by the internet, with emails and file transfers replacing letters.

In the 1990s the MFI Oberwolfach had to change its policy which resulted in limitations of the number of participants at conferences, and thus of younger academic visitors. When I first asked Wolfgang Schwarz about the prospect of starting separate conferences on elementary and analytic number theory particularly for young academics, he and several other colleagues convinced me to organize a low budget conference in Goslar. On his recommendation I was able to hire his postdoc Christian Elsholtz as assistant. In 2000, he and some student assistants helped to host that first ELAZ conference in Goslar, with 26 registered participants from five countries. In 2012, Schwarz and I were very pleased that the ELAZ conferences had developed so well, for the number of participants of the ELAZ conference organized by Jörn Steuding had risen to 71 participants from 27 countries.

Until 2012 Wolfgang Schwarz was full of health and strength, staying true to his high ideals, and following his example kept me going. I am deeply indebted to him for his steady support during more than 40 years.

The subsequent sections contain a survey of Schwarz's work on three interrelated topics belonging to the theory of arithmetic functions. They are chosen according to my own research interests and have been initiated and developed further by Wolfgang Schwarz, his students, and colleagues.

4 Inversion Theorems for Multiplicative Functions

The 1960s and 1970s have been important decades for the development of the theory of arithmetic functions, in particular, that of multiplicative and additive functions. In 1967, Wirsing [38] solved the Erdős–Wintner problem and proved that every real multiplicative function of modulus ≤ 1 has a mean-value, a result that is equivalent to the prime number theorem. In 1968, Halász [6] solved Wirsing's problem by determining the asymptotic behavior of the partial sums of the values of complex multiplicative functions of modulus ≤ 1 at arguments $n \leq x$. What these papers have in common is a simplification of the problem by replacing the original multiplicative function f with a simpler related one, coinciding with f on the set of sufficiently large primes only and neglecting the values at higher prime powers. In fact, there is a previous paper of Delange [2] from 1961, which introduces the notion of related multiplicative functions and gives some applications. In 1983, Indlekofer [10] proved a general mean value theorem for uniformly summable multiplicative functions.

In the 1970s, Schwarz considered this strategy under structural aspects and began to develop methods for transferring mean properties between complex valued multiplicative functions f and g. Let $\mathscr{M}$ denote the class of multiplicative functions.

From a more general point of view, Schwarz's approach may be described as follows: The deviation between arithmetic functions $f, g\colon \mathbb{N} \to \mathbb{C}$ with $g(1) \neq 0$ can be considered small if the Dirichlet series $\tilde{h}(s)$ of h (implicitly) defined by $f = g * h$ converges absolutely at $s = 1$. This is an ℓ^1-norm condition on h, which for $f, g \in \mathscr{M}$ is equivalent to

$$\sum_{p,k\geq 1} |h(p^k)|\, p^{-k} < \infty.$$

Here and in the sequel, the letter p always denotes primes. After a thorough analysis of Delange's result, Schwarz [21] uses the Wiener inversion theorem for power series for an elegant proof of an extension of Delange's result. Let $\mathscr{S}$ be Schwarz's class of multiplicative functions f bounded in mean, and satisfying the local conditions $f^2(p) \ll p^{1-\delta}, f(p^r) \ll c^r$ for $r \geq 2$ with some constants $\delta > 0$ and c, $1 \leq c < 2$. Denote by $\mathscr{D}$ the class of arithmetic functions $h\colon \mathbb{N} \to \mathbb{C}$ with absolutely convergent Dirichlet series $\tilde{h}(1)$.

Theorem (Schwarz [21]) Let $f, g \in \mathscr{S}$ satisfy

$$\sum_p |f(p) - g(p)|\, p^{-1} < \infty.$$

If no Euler product factor $\tilde{g}_p(s) = 1 + g(p)p^{-s} + g(p^2)p^{-2s} + \cdots$ of $\tilde{g}(s)$, p prime, has a zero in the closed half plane $\operatorname{Re} s \geq 1$, then $h := f * g^{-1} \in \mathscr{D}$. In particular, the existence of the mean value $M(g) = \lim_{x\to\infty} \left(x^{-1} \sum_{n\leq x} g(n)\right)$ implies that of $M(f) = \tilde{h}(1) \cdot M(g)$.

This theorem has some important applications, but also some undesirable restrictions concerning the above local conditions of Wirsing type (see Wirsing [37]) and, especially, the shortness of the class $\mathscr{S}$. In fact, the local conditions on f and g can be replaced with mean conditions extending $\mathscr{S}$ further, which yields some mean value applications (see [13]).

5 Collaborations with Spilker and Heppner

Due to the general importance of Wiener type inversion, the proof of the original Wiener inversion theorem [36] for Fourier series and power series was simplified by Gelfand's theory of commutative Banach algebras, extended to ordinary Dirichlet series by Hewitt and Williamson [8] and, moreover, to general Dirichlet series by Edwards [3].

When Spilker and Schwarz [33] began to inspect Gelfand's theory in the context of arithmetic functions, they found even shorter proofs of inversion theorems in commutative Banach spaces of arithmetic functions corresponding to generating power series, Fourier series, and Dirichlet series. In particular, their new approach to the inversion theorem for Dirichlet series, based on the Kronecker approximation theorem and the maximum principle for holomorphic functions, produced a density result interesting in itself.

Recall that, under pointwise addition and the Dirichlet convolution $*$, the class A of arithmetic functions $a\colon \mathbb{N} \to \mathbb{C}$ with finite ℓ^1-norm $\|a\| := \sum_{n=1}^{\infty} |a(n)| < \infty$ is a Banach algebra with unit ε, $\varepsilon(1) = 1$ and $\varepsilon(n) = 0$ for $n > 1$. The spectrum $\sigma(a)$ of $a \in A$ is the set of all $\lambda \in \mathbb{C}$ such that $a - \lambda\varepsilon$ is not invertible in A. Denote by $\mathbb{H} := \{s \in \mathbb{C} : \operatorname{Re} s > 0\} \subset \mathbb{C}$ the open right half plane.

Theorem (Schwarz–Spilker [33]) For every $a \in A$, $\tilde{a}(\mathbb{H})$ is dense in $\sigma(a)$.

As an application, Heppner and Schwarz [7] proved an inversion theorem for multiplicative functions or, equivalently, for Dirichlet series with multiplicative coefficient functions, which correspond to Euler products.

Theorem (Heppner–Schwarz [7]) The class

$$\mathscr{G} = \Big\{ g \in \mathscr{M} : \sum_p |g^2(p)|\, p^{-2} < \infty \text{ and } \sum_{p,k\geq 2} |g(p^k)|\, p^{-k} < \infty \Big\}$$

is a unital semigroup under the Dirichlet convolution $*$ with the multiplicative group

$$\mathscr{G}^* = \big\{ g \in \mathscr{G} : 0 \notin \tilde{g}_p(1 + \overline{\mathbb{H}}) \text{ for all } p \big\}.$$

The class $\mathscr{G}$ extends the Schwarz class $\mathscr{S}$ considerably by replacing the ℓ^1-norm on the image set $g(\mathbb{P})$ of the set $\mathbb{P}$ of primes with the ℓ^2-norm. Thus the above theorem of Heppner and Schwarz is a remarkable structural result. In particular, the rigid restrictions in Schwarz's relationship theorem from 1973 do not appear any longer.

Corollary (Heppner–Schwarz [7]) Let $f \in \mathscr{G}$, $g \in \mathscr{G}^*$ satisfy $\sum_p |f(p) - g(p)|\, p^{-1} < \infty$ and let h be defined by $f = g * h$. Then $\tilde{h}(1)$ converges absolutely.

In a survey paper [29, Problem 8.6] from 1985, and at conferences, Schwarz posed the problem of finding quantitative versions of this relationship theorem. He was very pleased to see the solution [14] and its arithmetic applications based on the investigation of suitable weight functions and Banach algebras of arithmetic functions with weighted norms.

It is worth mentioning that the proof of the above density theorem of Schwarz and Spilker from 1979 can be simplified by using the following maximum modulus principle for holomorphic functions of several variables, which seems to be little-known.

Lemma (Glöckner–Lucht [5]) Let $G = G_1 \times \cdots \times G_k$ with nonempty bounded regions $G_1, \ldots, G_k \subset \mathbb{C}$. If $f\colon \overline{G} \to \mathbb{C}$ is continuous on $\overline{G}$ and holomorphic on G, then $|f|$ takes its maximum value on $\partial G_1 \times \cdots \times \partial G_k$.

Its proof by induction uses the maximum modulus principle for holomorphic functions (of one variable) and the Weierstraß convergence theorem. The paper [5] contains a new proof of Edwards's inversion theorem [3] for general Dirichlet series in terms of complex valued functions, defined on additive arithmetic semigroups, and includes applications to Banach algebras of multidimensional Dirichlet series associated with arithmetic functions.

6 Ramanujan Expansions

In 1918, Ramanujan [19] introduced the sums of the ath powers of the nth roots of unity,

$$c_n(a) = \sum_{\substack{1\le \nu\le n\\ \gcd(\nu,n)=1}} e^{2\pi i\frac{a\nu}{n}} \qquad (a,n\in\mathbb{N}),$$

later called *Ramanujan sums*, and gave numerous examples of pointwise convergent series expansions of arithmetic functions $f\colon \mathbb{N}\to\mathbb{C}$ of the form

$$f(a) = \sum_{n=1}^{\infty} \hat{f}(n)\, c_n(a) \qquad (a\in\mathbb{N})$$

with suitable so-called Ramanujan coefficients $\hat{f}(n)$. Such representations are called Ramanujan expansions of f.

Well-known properties of the Ramanujan sums are:

(a) for any $n\in\mathbb{N}$ fixed, $c_n(a) = c_{\gcd(n,a)}(a)$ is an n-even function of a,
(b) for all $n,a\in\mathbb{N}$, $c_n(a) = \sum_{d\mid\gcd(n,a)} d\,\mu\left(\frac{n}{d}\right) \in\mathbb{R}$ holds,
(c) for any $a\in\mathbb{N}$ fixed, $c_n(a)$ is a multiplicative function of n.

Among Ramanujan's examples of expansions we find the evaluations

$$0 = \sum_{n=1}^{\infty} \frac{c_n(a)}{n} \quad\text{and}\quad -1 = \sum_{n=1}^{\infty} \frac{c_n(a)}{n}\log n \qquad (a\in\mathbb{N}),$$

which both are equivalent to the prime number theorem, in the latter case with nontrivial remainder term. In particular, the first example shows that Ramanujan expansions are not uniquely determined.

For a long time, Ramanujan expansions remained a mysterious topic in number theory. In 1932, Carmichael [1] suggested to find a Fourier analytic approach. In 1981, Hildebrand [9] showed by an inductive construction that every arithmetic function has a Ramanujan expansion. However, Hildebrand's expansions appear strange and have nothing in common with the "natural" ones displayed by Ramanujan.

In 1975, Knopfmacher [12, Chap. 7] presented a survey containing a general mean-value based concept for convergence of the above Ramanujan series in quadratic mean and, moreover, suggested to develop a new concept, which preserves and explains known expansions that do not fit in the mean-value based concept.

The problem of finding a general mean-value based approach to pointwise convergence remained open until Schwarz, encouraged by the progress of mean-value theorems for multiplicative functions, began to develop such a concept in 1972. In a series of papers [22–24, 27, 28] he considered the Ramanujan coefficients

$$\hat{g}(n) = \frac{M(gc_n)}{\varphi(n)}$$

of $g \in \mathscr{M}$, where φ is the Euler function, and proceeded in three steps, namely

1. determine suitable classes of arithmetic functions such that the above mean-values exist,
2. evaluate the Ramanujan coefficients,
3. prove pointwise convergence of the Ramanujan series to the "correct" value.

With technically intricate proofs he succeeded to verify the following

Theorem (Schwarz [26]) Let $g \in \mathscr{M}$ be bounded by 1. If $M(g) \neq 0$ exists then the Ramanujan coefficients $\hat{g}(n)$ exist for all $n \in \mathbb{N}$, and the respective Ramanujan series converges pointwise to g.

In 1980, Tuttas [34] extended Schwarz's result to the class $\mathscr{E}_2$ of multiplicative functions characterized by Elliott [4]. A further extension to the generalized Elliott class $\mathscr{E}^q$ with $q > 1$ follows from papers of Indlekofer [11] and Warlimont [35].

Schwarz's approach to pointwise convergent Ramanujan expansions is restricted to multiplicative functions having a mean-value and satisfying certain approximation conditions used by Schwarz and Spilker in [32] to define and explore suitable normed algebras of almost-even arithmetic functions. It does not explain the known Ramanujan expansions of, for instance, the divisor function $d(n)$ or the counting function $r(n)$ of the number of points $(a, b) \in \mathbb{Z}^2$ in a circle of radius $\sqrt{n}$.

In 1993, a new concept was established in [14] (see also [15] and [17]), which solved both problems to find a quantitative "weighted" version of the Heppner-Schwarz relationship theorem and a new concept of Ramanujan expansions. The latter is based on a weighted relationship between the Ramanujan sums and the Möbius function (see the survey paper [16]), and explains and preserves the previously "mysterious" Ramanujan expansions. Schwarz was very surprised and delighted. He said, if he could change the monograph *Arithmetical Functions* he would rewrite several chapters.

All of us who knew and worked with Wolfgang Schwarz are deeply indebted to him for his steady support, his friendship, and his ideas, which he kindly shared with us.

At Oberwolfach conferences on elementary and analytical number theory Paul Erdős loved to talk about God's Book containing the most beautiful mathematical theorems and their ultimate proofs. Let us think of Wolfgang Schwarz now happily studying The Book with all the wonderful results, to which he has contributed so much during his time on earth.

Acknowledgements The author thanks the Schwarz family for their great help with photos and data, Jürgen Spilker (Freiburg), Peter Bundschuh (Köln), Karl-Heinz Indlekofer (Paderborn), Jürgen Wolfart (Frankfurt), Jörn Steuding (Würzburg), Christian Elsholtz (Graz), for their memories of Wolfgang Schwarz's work and life at the universities of Freiburg and Frankfurt, Aleksandar Ivić (Belgrade) for communicating many details, the chairman Thomas Walter and members of the Schachclub Erlangen 48/88 for submitting archive-data, and Karl Dilcher (Halifax) and Friedemann Tuttas (Wiesbaden) for thoroughly proofreading the manuscript and valuable suggestions.

References

1. R.D. Carmichael, Expansions of arithmetical functions in infinite series. Proc. Lond. Math. Soc. **34**, 1–26 (1932)
2. H. Delange, Sur les fonctions arithmétiques multiplicatives. Ann. Scient. École Norm. Sup., 3^{e} série, **78**, 273–304 (1961)
3. D.A. Edwards, On absolutely convergent Dirichlet series. Proc. Am. Math. Soc. **8**, 1067–1074 (1957)
4. P.D.T.A. Elliott, A mean-value theorem for multiplicative functions. Proc. Lond. Math. Soc. **31**, 418–438 (1975)
5. H. Glöckner, L.G. Lucht, Weighted inversion of general Dirichlet series. Trans. Am. Math. Soc. **366**, 3275–3293 (2014)
6. G. Halász, Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen. Acta Math. Sci. Hung. **19**, 365–403 (1968)
7. E. Heppner, W. Schwarz, *Benachbarte multiplikative Funktionen*. Studies in Pure Mathematics (To the Memory of Paul Turán) (Birkhäuser, Basel, 1983), pp. 323–336
8. E. Hewitt, J.H. Williamson, Note on absolutely convergent Dirichlet series. Proc. Am. Math. Soc. **8**, 863–868 (1957)
9. A. Hildebrand, Über die punktweise Konvergenz von Ramanujan-Entwicklungen zahlentheoretischer Funktionen. Acta Arith. **44**, 109–140 (1984)
10. K.-H. Indlekofer, A mean-value theorem for multiplicative functions. Math. Z. **172**, 255–271 (1980)
11. K.-H. Indlekofer, Some remarks on almost-even and almost-periodic functions. Archiv Math. **37**, 353–358 (1981)
12. J. Knopfmacher, *Abstract Analytic Number Theory* (North Holland, Amsterdam, 1975); Reprint Dover, New York 1990
13. L.G. Lucht, Über benachbarte multiplikative Funktionen. Arch. Math. **30**, 40–48 (1978)
14. L.G. Lucht, An application of Banach algebra techniques to multiplicative functions. Math. Z. **214**, 287–295 (1993)
15. L.G. Lucht, Weighted relationship theorems and Ramanujan expansions. Acta Arith. **70**, 25–42 (1995)
16. L.G. Lucht, A survey of Ramanujan expansions. Int. J. Number Theory **6**(8), 1785–1799 (2010)
17. L.G. Lucht, K. Reifenrath, Weighted Wiener-Lévy theorems. Analytic Number Theory, in *Proceedings of a Conference in Honor of Heini Halberstam*, Urbana-Champaign, 1995, vol. 2 (Birkhäuser, Boston 1996), pp. 607–619
18. L.G. Lucht, W. Schwarz, Über die Lösungsanzahl der Gleichung $f(n) = \kappa n$ für gewisse Klassen multiplikativer Funktionen. Monatshefte Math. **81**, 213–216 (1976)
19. S. Ramanujan, On certain trigonometrical sums and their applications in the theory of numbers. Trans. Camb. Philos. Soc. **22**, 259–276 (1918)
20. W. Schwarz, *Einführung in Ergebnisse und Methoden der Primzahltheorie* (Bibliographisches Institut, Mannheim, 1969)

21. W. Schwarz, Eine weitere Bemerkung über multiplikative Funktionen. Colloq. Math. **28**, 81–89 (1973)
22. W. Schwarz, Ramanujan-Entwicklungen stark multiplikativer zahlentheoretischer Funktionen. Acta Arith. **22**, 329–338 (1973)
23. W. Schwarz, Ramanujan-Entwicklung stark multiplikativer Funktionen. J. Reine Angew. Math. **262/263**, 66–73 (1973)
24. W. Schwarz, Die Ramanujan-Entwicklung reellwertiger multiplikativer Funktionen vom Betrage kleiner oder gleich Eins. J. Reine Angew. Math. **271**, 171–176 (1974)
25. W. Schwarz, *Einführung in Siebmethoden der analytischen Zahlentheorie* (Bibliographisches Institut, Mannheim, 1974)
26. W. Schwarz, *Einführung in die Zahlentheorie* (Wissenschaftliche Buchgesellschaft, Darmstadt, 1975)
27. W. Schwarz, Über die Ramanujan-Entwicklung multiplikativer Funktionen. Acta Arith. **27**, 269–279 (1975)
28. W. Schwarz, Fourier-Ramanujan-Entwicklungen zahlentheoretischer Funktionen und Anwendungen, in *Festschrift der Wissenschaftlichen Gesellschaft an der Johann-Wolfgang-Goethe-Universität Frankfurt am Main* (Steiner Verlag, Wiesbaden, 1981), pp. 399–415
29. W. Schwarz, Remarks on the theorem of Elliott and Daboussi, and applications, in *Elementary and Analytic Theory of Numbers* (Warsaw, 1982), 463–498, Banach Center Publication, vol. 17 (PWN, Warsaw, 1985)
30. W. Schwarz (Hrsg.), *Aus der Geschichte der Frankfurter Mathematik*. Festschrift zu den 100. Geburtstagen von Ruth Moufang, Gottfried Köthe, Wolfgang Franz, Frankfurt am Main, 2005, p. 203; Universitätsarchiv Frankfurt am Main, Senkenberganlage 31–33, 60325 Frankfurt am Main
31. W. Schwarz, J. Spilker, Eine Bemerkung zur Charakterisierung der fast-periodischen multiplikativen zahlentheoretischen Funktionen mit von Null verschiedenem Mittelwert. Analysis **3**, 205–216 (1983)
32. W. Schwarz, J. Spilker, *Arithmetical Functions* (Cambridge University Press, Cambridge, 1994)
33. J. Spilker, W. Schwarz, Wiener-Lévy-Sätze für absolut konvergente Reihen. Arch. Math. **32**, 267–275 (1979)
34. F. Tuttas, Über die Entwicklung multiplikativer Funktionen nach Ramanujan-Summen. Acta Arith. **36**, 257–270 (1980)
35. R. Warlimont, Ramanujan expansions of multiplicative functions. Acta Arith. **42**, 112–120 (1983)
36. N. Wiener, Tauberian theorems. Ann. Math. (2) **33**, 1–100 (1932)
37. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. Math. Ann. **143**, 75–102 (1961)
38. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen II. Acta Math. Acad. Hung. **18**, 411–467 (1967)

Dynamical Systems and Uniform Distribution of Sequences

Manfred G. Madritsch and Robert F. Tichy

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract We give a survey on classical and recent applications of dynamical systems to number theoretic problems. In particular, we focus on normal numbers, also including computational aspects. The main result is a sufficient condition for establishing multidimensional van der Corput sets. This condition is applied to various examples.

Keywords Dynamical systems • Uniform distribution • van der Corput set

2010 Mathematics subject classification: Primary 11J71; Secondary 11K38

1 Dynamical Systems in Number Theory

In the last decades dynamical systems became very important for the development of modern number theory. The present paper focuses on Furstenberg's refinements of Poincaré's recurrence theorem and applications of these ideas to Diophantine problems.

A (measure-theoretic) dynamical system is formally given as a quadruple $(X, \mathfrak{B}, \mu, T)$, where $(X, \mathfrak{B}, \mu)$ is a probability space with σ-algebra $\mathfrak{B}$ of measurable sets and μ a probability measure; $T: X \to X$ is a measure-preserving

M.G. Madritsch
Institut Elie Cartan de Lorraine, Université de Lorraine, UMR 7502, Vandoeuvre-lès-Nancy F-54506, France

CNRS, Institut Elie Cartan de Lorraine, UMR 7502, Vandoeuvre-lès-Nancy F-54506, France
e-mail: manfred.madritsch@univ-lorraine.fr

R.F. Tichy (✉)
Department for Analysis and Number Theory, Graz University of Technology, A-8010 Graz, Austria
e-mail: tichy@tugraz.at

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_17

transformation on this space, i.e. $\mu(T^{-1}A) = \mu(A)$ for all measurable sets $A \in \mathfrak{B}$. In the theory of dynamical systems, properties of the iterations of the transformation T are of particular interest. For this purpose we only consider invertible transformations and call such dynamical systems invertible.

The first property, we consider, originates from Poincaré's famous recurrence theorem (see Theorem 1.4 of [32] or Theorem 2.11 of [13]) saying that starting from a set A of positive measure $\mu(A) > 0$ and iterating T yields infinitely many returns to A. More generally, we call a subset $\mathcal{R} \subset \mathbb{N}$ of the positive integers a set of recurrence if for all invertible dynamical systems and all measurable sets A of positive measure $\mu(A) > 0$ there exists $n \in \mathcal{R}$ such that $\mu(A \cap T^{-n}A) > 0$. Then Poincaré's recurrence theorem means that $\mathbb{N}$ is a set of recurrence.

A second important theorem for dynamical systems is Birkhoff's ergodic theorem (see Theorem 1.14 of [32] or Theorem 2.30 of [13]). We call T ergodic if the only invariant sets under T are sets of measure 0 or of measure 1, i.e. $T^{-1}A = A$ implies $\mu(A) = 0$ or $\mu(A) = 1$. Then Birkhoff's ergodic theorem connects average in time with average in space, i.e.,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f \circ T^n(x) = \int_X f(x) d\mu(x)$$

for all $f \in L^1(X, \mu)$ and μ-almost all $x \in X$.

Let us explain an important application of this theorem to number theory. For $q \geq 2$ a positive integer, consider $T\colon [0,1) \to [0,1)$ defined by $T(x) = \{qx\}$, where $\{t\} = t - \lfloor t \rfloor$ denotes the fractional part of t. If $x \in \mathbb{R}$ is given by its q-ary digit expansion $x = \lfloor x \rfloor + \sum_{j=1}^{\infty} a_j(x) q^{-j}$, then the digits $a_j(x)$ can be computed by iterating this transformation T: $a_j(x) = d$ if $T^{j-1}x \in \left[\frac{d}{q}, \frac{d+1}{q}\right)$ with $d \in \{0, 1, \ldots, q-1\}$. Moreover, since $a_j(Tx) = a_{j+1}(x)$ for $j \geq 1$ the transformation T can be seen as a left shift of the expansion.

Now we call a real number x simply normal in base q if

$$\lim_{\mathbb{N}\to\infty} \frac{1}{N} \#\{j \leq N\colon a_j(x) = d\} = \frac{1}{q}$$

for all $d = 0, \ldots, q-1$, i.e., all digits d appear asymptotically with equal frequencies $1/q$. A number x is called q-normal if it is simply normal with respect to all bases $q, q^2, q^3, \ldots$. This is equivalent to the fact that the sequence $(\{q^n x\})_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 (for short: u.d. mod 1), which also means that all blocks $d_1, d_2, \ldots, d_L$ of subsequent digits appear in the expansion of x asymptotically with the same frequency q^{-L} (cf. [8, 12, 16]). For completeness, let us give here one possible definition of u.d. sequences (x_n): a sequence of real numbers x_n is called u.d. mod 1 if for all continuous functions $f : [0,1] \to \mathbb{R}$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x) dx. \tag{1.1}$$

Note, that by Weyl's criterion the class of continuous functions can be replaced by trigonometric functions $e(hx) = e^{2\pi ihx}$, $h \in \mathbb{N}$ or by characteristic functions $1_I(x)$ of intervals $I = [a, b)$. Applying Birkhoff's ergodic theorem shows that Lebesgue almost all real numbers are q-normal in any base $q \geq 2$. Defining a real number to be absolutely normal if it is q-normal for all bases $q \geq 2$, this immediately yields that almost all real numbers are absolutely normal.

In particular, this shows the existence of absolutely normal numbers. However, it is a different story to find constructions of (absolutely) normal numbers. It is a well-known difficult open problem to show that important numbers like $\sqrt{2}$, $\ln 2$, e, π etc. are simply normal with respect to some given base $q \geq 2$. A much easier task is to give constructions of q-normal numbers for fixed base q. Champernowne [9] proved that

$$0.1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\ldots$$

is normal to base 10 and later this type of constructions was analyzed in detail. So, for instance, for arbitrary base $q \geq 2$

$$0.\langle \lfloor g(1) \rfloor \rangle_q \, \langle \lfloor g(2) \rfloor \rangle_q \ldots$$

is q-normal, where $g(x)$ is a non-constant polynomial with real coefficients and the q-normal number is constructed by concatenating the q-ary digit expansions $\langle \lfloor g(n) \rfloor \rangle_q$ of the integer parts of the values $g(n)$ for $n = 1, 2, \ldots$. These constructions were extended to more general classes of functions g (replacing the polynomials) (see [11, 18, 19, 22, 23, 29]) and the concatenation of $\langle [g(p)] \rangle_q$ along prime numbers instead of the positive integers (see [10, 17, 18, 24]).

All such constructions depend on the choice of the base number $q \geq 2$, and thus they are not suitable for constructing absolutely normal numbers. A first attempt to construct absolutely normal numbers is due to Sierpinski [30]. However, Turing [31] observed that Sierpinski's "construction" does not yield a computable number, thus it is not based on a recursive algorithm. Furthermore, Turing gave an algorithm for a construction of an absolutely normal number. This algorithm is very slow and, in particular, not polynomially in time. It is very remarkable that Becher et al. [2] established a polynomial time algorithm for the construction of absolutely normal numbers. However, there remain various questions concerning the analysis of these algorithms. The discrepancy of the corresponding sequences is not studied and the order of convergence of the expansion is very slow and should be investigated in detail. Furthermore, digital expansions with respect to linear recurring base sequences seem appropriate to be included in the study of absolute normality from a computational point of view.

Let us now return to Poincaré's recurrence theorem which shortly states that the set $\mathbb{N}$ of positive integers is a recurrence set. In the 1960s various stronger concepts were introduced:

1. $\mathcal{R} \subseteq \mathbb{N}$ is called a nice recurrence set if for all invertible dynamical systems and all measurable sets A of positive measure $\mu(A) > 0$ and all $\varepsilon > 0$, there exist infinitely many $n \in \mathcal{R}$ such that

$$\mu(A \cap T^{-n}A) > \mu(A)^2 - \varepsilon.$$

2. $\mathcal{H} \subseteq \mathbb{N}$ is called a van der Corput set (for short: vdC set) if the following implications holds:

$$(x_{n+h} - x_n)_{n\in\mathbb{N}} \text{ is u.d. mod 1 for all } h \in \mathcal{H} \Longrightarrow (x_n)_{n\in\mathbb{N}} \text{ is u.d. mod 1.}$$

Clearly, any nice recurrence set is a recurrence set. By van der Corput's difference theorem (see [12, 16]) the set $\mathcal{H} = \mathbb{N}$ of positive integers is a vdC set. Kamae and Mendès-France [15] proved that any vdC set is a nice recurrence set. Ruzsa [25] conjectured that any recurrence set is also a vdC set. An important tool in the analysis of recurrence sets is their equivalence with intersective (or difference) sets established by Bertrand-Mathis [5]. We call a set $\mathcal{I}$ intersective if for each subset $E \subseteq \mathbb{N}$ of positive (upper) density, there exists $n \in \mathcal{I}$ such that $n = x - y$ for some $x, y \in E$. Here the upper density of E is defined as usual by

$$\overline{d}(E) = \limsup_{N\to\infty} \frac{\#(E \cap [1, N])}{N}.$$

Bourgain [7] gave an example of an intersective set which is not a vdC set, hence contradicting the above mentioned conjecture of Ruzsa.

Furstenberg [14] proved that the values $g(n)$ of a polynomial $g \in \mathbb{Z}[x]$ with $g(0) = 0$ form an intersective set and later it was shown by Kamae and Mendès-France [15] that this is a vdC set, too. It is also known that for fixed $h \in \mathbb{Z}$ the set of shifted primes $\{p \pm h : p \text{ prime}\}$ is a vdC set if and only if $h = \pm 1$. [20, Corollary 10]. This leads to interesting applications to additive number theory, for instance to new proofs and variants of theorems of Sárközy [26–28]. A general result concerning intersective sets related to polynomials along primes is due to Nair [21].

In the present paper we want to extend the concept of recurrence sets, nice recurrence sets, and vdC sets to subsets of $\mathbb{Z}^k$, following the program of Bergelson and Lesigne [3] and our earlier paper [4]. In Sect. 2 we summarize basic facts concerning these concepts, including general relations between them and counter examples. Section 3 is devoted to a sufficient condition for establishing the vdC property. In the final Sect. 4 we collect various examples and give some new applications.

2 van der Corput Sets

In this section we provide various equivalent definitions of van der Corput sets in $\mathbb{Z}^k$. In particular, we give four different definitions, which are k-dimensional variants of the one-dimensional definitions, whose equivalence is due to Ruzsa [25]. These generalizations were established by Bergelson and Lesigne [3]. Then we present a set, which is not a vdC set in order to give some insight into the structure of vdC sets. Finally, we define the higher-dimensional variant of nice recurrence sets.

2.1 Characterization via Uniform Distribution

Similar to above we first define a van der Corput set (vdC set for short) in $\mathbb{Z}^k$ via uniform distribution.

Definition 2.1 *A subset $\mathcal{H} \subset \mathbb{Z}^k \setminus \{0\}$ is a vdC set if any family $(x_{\mathbf{n}})_{\mathbf{n}\in\mathbb{N}^k}$ of real numbers is u.d. mod* 1 *provided that it has the property that for all $\mathbf{h} \in \mathcal{H}$ the family $(x_{\mathbf{n}+\mathbf{h}} - x_{\mathbf{n}})_{\mathbf{n}\in\mathbb{N}^k}$ is u.d. mod* 1.

Here the property of u.d. mod 1 for the multi-indexed family $(x_{\mathbf{n}})_{\mathbf{n}\in\mathbb{N}^k}$ is defined via a natural extension of 1.1:

$$\lim_{N_1,N_2,\ldots,N_k\to+\infty} \frac{1}{N_1N_2\cdots N_k} \sum_{0\le\mathbf{n}<(N_1,N_2,\ldots,N_k)} f(x_{\mathbf{n}}) = \int_0^1 f(x)dx \tag{2.1}$$

for all continuous functions $f : [0, 1] \to \mathbb{R}$. Here in the limit $N_1, N_2, \ldots, N_k$ are tending to infinity independently and $<$ is defined componentwise.

Using the k-dimensional variant of van der Corput's inequality we could equivalently define a vdC set as follows:

Definition 2.2 *A subset $\mathcal{H} \subset \mathbb{Z}^k \setminus \{0\}$ is a van der Corput set if for any family $(u_{\mathbf{n}})_{n\in\mathbb{Z}^k}$ of complex numbers of modulus* 1 *such that*

$$\forall \mathbf{h} \in \mathcal{H}, \quad \lim_{N_1,N_2,\ldots,N_k\to+\infty} \frac{1}{N_1N_2\cdots N_k} \sum_{0\le\mathbf{n}<(N_1,N_2,\ldots,N_k)} u_{\mathbf{n}+\mathbf{h}}\overline{u_{\mathbf{n}}} = 0$$

the relation

$$\lim_{N_1,N_2,\ldots,N_k\to+\infty} \frac{1}{N_1N_2\cdots N_k} \sum_{0\le\mathbf{n}<(N_1,N_2,\ldots,N_k)} u_{\mathbf{n}} = 0$$

holds.

2.2 Trigonometric Polynomials and Spectral Characterization

The first two definitions are not very useful for proving or disproving that a set $\mathcal{H}$ is a vdC set. Similar to the one-dimensional case the following spectral characterization involving trigonometric polynomials is a better tool.

Theorem 2.3 ([3, Proposition 1.18]) *A subset $\mathcal{H} \subset \mathbb{Z}^k \setminus \{0\}$ is a van der Corput set if and only if for all $\varepsilon > 0$, there exists a real trigonometric polynomial P on the k-torus $\mathbb{T}^k$ whose spectrum is contained in $\mathcal{H}$ and which satisfies $P(0) = 1$, $P \geq -\varepsilon$.*

The set of polynomials fulfilling the last theorem for a given ε forms a convex set. Moreover the conditions may be interpreted as some infimum. Therefore we might expect some dual problem, which is actually provided by the following theorem. For details see Bergelson and Lesigne [3] or Montgomery [20].

Theorem 2.4 ([3, Theorem 1.8]) *Let $\mathcal{H} \subset \mathbb{Z}^k \setminus \{0\}$. Then $\mathcal{H}$ is a van der Corput set if and only if for any positive measure σ on the k-torus $\mathbb{T}^k$ such that, for all $\mathbf{h} \in \mathcal{H}$, $\hat{\sigma}(\mathbf{h}) = 0$, this implies $\sigma(\{(0, 0, \dots, 0)\}) = 0$.*

2.3 Examples

The structure of vdC sets is better understood by first giving a counter example. The following lemma shows to be very useful in the construction of counter examples.

Lemma 2.5 *Let $\mathcal{H} \subset \mathbb{N}$. If there exists $q \in \mathbb{N}$ such that the set $\mathcal{H} \cap q\mathbb{N}$ is finite, then the set $\mathcal{H}$ is not a vdC set.*

Proof The proof is a combination of the following two observations of Ruzsa [25] (see Theorem 2 and Corollary 3 of [20]):

1. Let $m \in \mathbb{N}$. The sets $\{1, \dots, m\}$ and $\{n \in \mathbb{N} : m \nmid n\}$ are both not vdC sets.
2. Let $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2 \subset \mathbb{N}$. If $\mathcal{H}$ is a vdC set, then $\mathcal{H}_1$ or $\mathcal{H}_2$ also has to be a vdC set.

Suppose there exists a $q \in \mathbb{N}$ such that $\mathcal{H} \cap q\mathbb{N}$ is finite. Then we may split $\mathcal{H}$ into the sets $\mathcal{H} \cap q\mathbb{N}$ and $\mathcal{H} \setminus q\mathbb{N}$. The first one is finite and the second one contains no multiples of q. Therefore both are not vdC sets and hence $\mathcal{H}$ is not a vdC set.

The first counter example deals with arithmetic progressions.

Lemma 2.6 *Let $a, b \in \mathbb{N}$. If the set $\{an + b : n \in \mathbb{N}\}$ is a vdC set, then $a \mid b$.*

Proof Let $b \in \mathbb{N}$ and $\mathcal{H} = \{an + b : n \in \mathbb{N}\}$ be a vdC set. Then by Lemma 2.5 we must have

$$an + b \equiv b \equiv 0 \bmod a \quad \text{infinitely often.}$$

This implies that $a \mid b$.

The sufficiency (and also the necessity) of the requirement $a \mid b$ follows from the following result of Kamae and Mendès-France [15] (cf. Corollary 9 of [20]).

Lemma 2.7 *Let $P(z) \in \mathbb{Z}[z]$ and suppose that $P(z) \to +\infty$ as $z \to +\infty$. Then $\mathcal{H} = \{P(n) > 0 : n \in \mathbb{N}\}$ is a vdC set if and only if for every positive integer q the congruence $P(z) \equiv 0 \pmod{q}$ has a root.*

Now we want to establish a similar result for sets of the form $\{ap + b : p \text{ prime}\}$. In this case the following result is due to Bergelson and Lesigne [3] which is a generalization of the case $f(x) = x$ due to Kamae and Mendès-France [15].

Lemma 2.8 ([3, Proposition 1.22]) *Let f be a (non zero) polynomial with integer coefficients and zero constant term. Then the sets $\{f(p-1) : p \in \mathbb{P}\}$ and $\{f(p+1) : p \in \mathbb{P}\}$ are vdC sets in $\mathbb{Z}$.*

We show the converse direction.

Lemma 2.9 *Let a and b be nonzero integers. Then the set $\{ap + b : p \in \mathbb{P}\}$ is a vdC set if and only if $|a| = |b|$, i.e., $ap + b = a(p \pm 1)$.*

Proof It is clear from Lemma 2.8 that $\{ap + b : p \in \mathbb{P}\}$ is a vdC set if $|a| = |b|$.

On the contrary a combination of Lemma 2.5 and Lemma 2.6 yields that $a \mid b$. Now we consider the sequence modulo b. Then by Lemma 2.5 we get that

$$ap + b \equiv ap \equiv 0 \bmod b \quad \text{infinitely often.}$$

Since $(p, b) > 1$ only holds for finitely many primes p we must have $b \mid a$. Combining these two requirements yields $|a| = |b|$.

3 A Sufficient Condition

In this section we want to formulate a general sufficient condition which provides us with a tool to show for plenty of different examples that they generate a vdC set. This is a generalization of the conditions of Kamae and Mendès-France [15] and Bergelson and Lesigne [3]. Before stating the condition we need an auxiliary lemma.

Lemma 3.1 ([3, Corollary 1.15]) *Let d and e be positive integers, and let L be a linear transformation from $\mathbb{Z}^d$ into $\mathbb{Z}^e$ (represented by an $e \times d$ matrix with integer entries). Then the following assertions hold:*

1. *If D is a vdC set in $\mathbb{Z}^d$ and if $0 \notin L(D)$, then $L(D)$ is a vdC set in $\mathbb{Z}^e$.*
2. *Let $D \subseteq \mathbb{Z}^d$. If the linear map L is one-to-one, and if $L(D)$ is a vdC set in $\mathbb{Z}^e$, then D is a vdC set in $\mathbb{Z}^d$.*

Our main tool is the following general result. Applications are given in the next section.

Proposition 3.2 *Let $g_1, \dots, g_k \colon \mathbb{N} \to \mathbb{Z}$ be arithmetic functions. Suppose that $g_{i_1}, \dots, g_{i_m}$ is a basis of the $\mathbb{Q}$-vector space* $\operatorname{span}(g_1, \dots, g_k)$. *For each $q \in \mathbb{N}$, we introduce*

$$D_q := \left\{(g_{i_1}(n), \dots, g_{i_m}(n) \colon n \in \mathbb{N} \text{ and } q! \mid g_{i_j}(n) \text{ for all } j = 1, \dots, m\right\}.$$

Suppose further that, for every q, there exists a sequence $(h_n^{(q)})_{n\in\mathbb{N}}$ in D_q such that, for all $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{R}^m \setminus \mathbb{Q}^m$, the sequence $(h_n^{(q)} \cdot \mathbf{x})_{n\in\mathbb{N}}$ is uniformly distributed mod 1. *Then*

$$\tilde{D} := \{(g_1(n), \dots, g_k(n)) \colon n \in \mathbb{N}\} \in \mathbb{Z}^k$$

is a vdC set.

Proof We first show that the set

$$D := \{(g_{i_1}(n), \dots, g_{i_m}(n)) \colon n \in \mathbb{N}\}$$

is a vdC set in $\mathbb{Z}^m$. For $q, N \in \mathbb{N}$ we define a family of trigonometric polynomials

$$P_{q,N} := \frac{1}{N} \sum_{n=1}^{N} e\left(h_n^{(q)} \cdot \mathbf{x}\right).$$

By hypothesis, $\lim_{N\to\infty} P_{q,N}(x) = 0$ for $x \notin \mathbb{Q}^m$. For fixed q there exists a subsequence $(P_{q,N'})$ which converges pointwise to a function g_q. Since $g_q(x) = 1$ (for $x \in \mathbb{Q}^m$ and q sufficiently large) and $g_q(x) = 0$ (for $x \notin \mathbb{Q}^m$), the sequence (g_q) is pointwise convergent to the indicator function of $\mathbb{Q}^m$. For a positive measure σ on the m-dimensional torus with vanishing Fourier transform $\hat{\sigma}$ on D, we have $\int P_{q,N} \mathrm{d}\sigma = 0$ for all q, N. Thus $\sigma(\mathbb{Q}^m) = 0$ follows from the dominating convergence theorem, obviously $\sigma(\{0, 0, \dots, 0\}) = 0$, and thus D is a vdC set.

In order to prove that $\tilde{D}$ is a vdC set we apply Lemma 3.1 twice. Since $g_{i_1}, \dots, g_{i_m}$ is a base of $\operatorname{span}(g_1, \dots, g_k)$, we can write each g_j as a linear combination (with rational coefficients) of $g_{i_1}, \dots, g_{i_m}$. Multiplying with the common denominator of the coefficients yields

$$a_j g_j = b_{j,1} g_{i_1} + \cdots + b_{j,m} g_{i_m}$$

for $j = 1, \dots, k$ and certain $a_j, b_{j,\ell} \in \mathbb{Z}$. Considering the transformation $L \colon \mathbb{Z}^m \to \mathbb{Z}^k$ given by the matrix $(b_{j,\ell})$ and applying part (1) of Lemma 3.1 shows that

$$\{(a_1 g_1(n), \dots, a_k g_k(n)) \colon n \in \mathbb{N}\}$$

is a vdC set for certain integers $a_1, \dots, a_k$.

Now consider the transformation $\tilde{L}\colon \mathbb{Z}^k \to \mathbb{Z}^k$ given by the $k \times k$ diagonal matrix with entries $a_1, \dots, a_k$ in the diagonal. Then by part (2) of Lemma 3.1 also $\tilde{D}$ is a vdC set and the proposition is proved.

4 Various Examples and Applications to Additive Problems

In this section we consider multidimensional variants of prime powers, entire functions and $x^\alpha \log^\beta x$ sequences.

4.1 Prime Powers

In a recent paper the authors together with Bergelson, Kolesnik, and Son [4] consider sets of the form

$$\{(\alpha_1(p_n \pm 1)^{\theta_1}, \dots, \alpha_k(p_n \pm 1)^{\theta_k})\colon n \in \mathbb{N}\},$$

where $\alpha_i, \beta_i \in \mathbb{R}$ and $p_n \in \mathcal{P}$ runs over all prime numbers. These sets are vdC, however, we missed the treatment of a special case in the proof. In particular, if for some $i \neq j$ the exponents satisfy $\theta_i = \theta_j =: \theta$, then the vector (p_n^θ, p_n^θ) is not uniformly distributed mod 1.

Here we close this gap.

Theorem 4.1 *If α_i are positive integers and β_i are positive and non-integers, then*

$$D_1 = \{\big((p-1)^{\alpha_1}, \cdots, (p-1)^{\alpha_k}, [(p-1)^{\beta_1}], \cdots, [(p-1)^{\beta_\ell}]\big)\,|\,p \in \mathcal{P}\},$$

and

$$D_2 = \{\big((p+1)^{\alpha_1}, \cdots, (p+1)^{\alpha_k}, [(p+1)^{\beta_1}], \cdots, [(p+1)^{\beta_\ell}]\big)\,|\,p \in \mathcal{P}\}$$

are vdC sets in $\mathbb{Z}^{k+\ell}$.

Proof Since x^{θ_1} and x^{θ_2} are $\mathbb{Q}$-linear dependent for all $x \in \mathbb{Z}$ if and only if $\theta_1 = \theta_2$, an application of Proposition 3.2 yields that it suffices to consider the case where all exponents are different. However, this follows by the same arguments as in the proof of Theorem 4.1 in [4].

4.2 Entire Functions

In this section we consider entire functions of bounded logarithmic order. We fix a transcendental entire function f and denote by $S(r) := \max_{|z|\le r} |f(z)|$. Then we call λ the logarithmic order of f if

$$\limsup_{r\to\infty} \frac{\log S(r)}{\log r} = \lambda.$$

The central tool is the following result of Baker [1].

Theorem 4.2 ([1, Theorem 2]) *Let f be a transcendental entire function of logarithmic order $1 < \lambda < \frac{4}{3}$. Then the sequence*

$$(f(p_n))_{n\ge 1}$$

is uniformly distributed mod 1.

Our second example of a class of vdC sets is the following.

Theorem 4.3 *Let $f_1, \dots, f_k$ be entire functions with distinct logarithmic orders $1 < \lambda_1, \lambda_2, \dots, \lambda_k < \frac{4}{3}$, respectively. Then the set*

$$D := \{(\lfloor f_1(p_n)\rfloor, \dots, \lfloor f_k(p_n)\rfloor) : n \in \mathbb{N}\}$$

is a vdC set.

Proof We enumerate $D = (\mathbf{d}_n)_{n\ge 1}$, where

$$\mathbf{d}_n := (\lfloor f_1(p_n)\rfloor, \dots, \lfloor f_k(p_n)\rfloor).$$

First we show that for every $q \in \mathbb{N}$ the set

$$D^{(q)} := \{(d_1, \dots, d_k) \in D : q \mid d_i\}$$

has positive relative density in D. We note that if $0 \le \left\{\frac{f_i(p_n)}{q}\right\} < \frac{1}{q}$ for $1 \le i \le k$, then $\mathbf{d}_n \in D^{(q)}$. By Theorem 4.2 the sequence

$$\left(\left(\frac{f_1(p_n)}{q}, \dots, \frac{f_k(p_n)}{q}\right)\right)_{n\ge 1}$$

is uniformly distributed and thus $D^{(q)}$ has positive density in D.

For each $q \in \mathbb{N}$ we enumerate the elements of $D^{(q!)} = (\mathbf{d}_n^{(q!)})_{n\ge 1}$, such that $\left|\mathbf{d}_n^{(q!)}\right|$ is increasing. Since the logarithmic orders are distinct we immediately get that the functions f_i are $\mathbb{Q}$-linearly independent. Thus by Proposition 3.2 it is sufficient to

show that for all $q \in \mathbb{N}$ and all $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{R}^k \setminus \mathbb{Q}^k$ the sequence $(\mathbf{d}_n^{(q!)} \cdot \mathbf{x})_{n \geq 1}$ is u.d. mod 1.

Using the orthogonality relations for additive characters we get for any nonzero integer h that

$$\frac{1}{\left|\{n \leq N : \mathbf{d}_n \in D^{(q!)}\}\right|} \sum_{n \leq N} e\left(h\left(d_n^{(q!)} \cdot \mathbf{x}\right)\right)$$

$$= \frac{1}{\left|\{n \leq N : \mathbf{d}_n \in D^{(q!)}\}\right|} \frac{1}{(q!)^k} \sum_{j_1=1}^{q!} \cdots \sum_{j_k=1}^{q!} \frac{1}{N} \sum_{n \leq N} e\left(d_n \cdot \left(h\mathbf{x} + \left(\frac{j_1}{q!}, \ldots, \frac{j_k}{q!}\right)\right)\right).$$

The innermost sum is of the form

$$\sum_{n \leq N} e(g(p_n)),$$

with $g(x) = \sum_{i=1}^k \alpha_i \lfloor f_i(x) \rfloor$ for a certain $(\alpha_1, \ldots, \alpha_k) \in \mathbb{R}^k \setminus \mathbb{Q}^k$.

By relabeling the terms we may suppose that there exists an ℓ such that $\alpha_1, \ldots, \alpha_\ell \notin \mathbb{Q}$ and $\alpha_{\ell+1}, \ldots, \alpha_k \in \mathbb{Q}$. Furthermore we may write $\alpha_j = \frac{a_j}{q}$ for $\ell + 1 \leq j \leq m$. Then

$$e(g(p_n)) = e\left(\sum_{i=1}^k \alpha_k \lfloor f_i(p_n) \rfloor\right) = \prod_{j=1}^{\ell} s_j(\alpha_j f_j(p_n), f_j(p_n)) \prod_{j=\ell+1}^{k} t_j(\lfloor f_j(p_n) \rfloor),$$

where $s_j(x, y) = e(x - \{y\}\alpha_j)$ $(1 \leq j \leq \ell)$ and $t_j(z) = e\left(a_j \frac{z}{q}\right)$ $(\ell + 1 \leq j \leq k)$.

Since $s_j(x, y)$ is Riemann-integrable on $\mathbb{T}^2$ for $j = 1, \ldots, \ell$ and $t_j(z)$ is continuous on $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, the function $\prod_{j=1}^{\ell} s_j \prod_{j=\ell+1}^{k} t_j$ is Riemann-integrable on $\mathbb{T}^{2\ell} \times \mathbb{Z}_q^{k-\ell}$.

Now an application of Theorem 4.2 yields that for any $u \in \mathbb{N}$ the sequence

$$\left(\alpha_1 f_1(p_n), f_1(p_n), \ldots, \alpha_\ell f_\ell(p_n), f_\ell(p_n), \frac{f_{\ell+1}(p_n)}{u}, \ldots, \frac{f_k(p_n)}{u}\right)_{n \geq 1}$$

is u.d. in $\mathbb{T}^{2\ell} \times \mathbb{T}^{k-\ell}$. Since $\lfloor x \rfloor \equiv a \pmod q$ is equivalent to $\frac{x}{q} \in [\frac{a}{q}, \frac{a+1}{q}]$, we deduce that

$$(\alpha_1 f_1(p_n), f_1(p_n), \ldots, \alpha_\ell f_\ell(p_n), f_\ell(p_n), \lfloor f_{\ell+1}(p_n) \rfloor, \ldots, \lfloor f_k(p_n) \rfloor)_{n \geq 1}$$

is u.d. in $\mathbb{T}^{2\ell} \times \mathbb{Z}_q^{k-\ell}$, and Weyl's criterion implies that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} e\left(\sum_{i=1}^{k} \alpha_i \lfloor f_i(p_n)\rfloor\right) = 0,$$

proving the theorem.

4.3 Functions of the Form $x^\alpha \log^\beta x$

In the one-dimensional case Boshernitzan et al. [6] showed, among other result, that these sets are vdC sets. Our aim is to show an extended version for the k-dimensional case. Therefore we use the following general criterion, which is a combination of Fejer's theorem and van der Corput's difference theorem.

Theorem 4.4 ([16, Theorem 3.5]) *Let $f(x)$ be a function defined for $x > 1$ that is k-times differentiable for $x > x_0$. If $f^{(k)}(x)$ tends monotonically to 0 as $x \to \infty$ and if $\lim_{x\to\infty} x\left|f^{(k)}(x)\right| = \infty$, then the sequence $(f(n))_{n\ge1}$ is u.d. mod 1.*

Applying this theorem we get the following

Corollary 4.5 *Let $\alpha \neq 0$ and*

- *either $\sigma > 0$ not an integer and $\tau \in \mathbb{R}$ arbitrary*
- *or $\sigma > 0$ an integer and $\tau \in \mathbb{R} \setminus [0, 1]$.*

Then the sequence $(\alpha n^\sigma \log^\tau n)_{n\ge2}$ is u.d. mod 1.

Our third example is the following class of vdC sets.

Theorem 4.6 *Let $\alpha_1, \dots, \alpha_k > 0$ and $\beta_1, \dots, \beta_k \in \mathbb{R}$, such that $\beta_i \notin [0, 1]$ whenever $\alpha_i \in \mathbb{Z}$ for $i = 1, \dots, k$. Then the set*

$$D := \{(\lfloor n^{\alpha_1} \log^{\beta_1} n\rfloor, \dots, \lfloor n^{\alpha_k} \log^{\beta_k} n\rfloor) : n \in \mathbb{N}\}$$

is a vdC set.

Proof Following the same arguments as is the proof of Theorem 4.3 and replacing the uniform distribution result for entire functions (Theorem 4.3) by the corresponding result for $n^\alpha \log^\beta n$ sequences (Corollary 4.5) yields the proof.

Acknowledgements This research work was done when the first author was a visiting professor at the Department of Analysis and Number Theory at Graz University of Technology. The author thanks the institution for its hospitality. For the realization of the present paper the first author received support from the Conseil Régional de Lorraine.

The second author acknowledges support of the project F 5510-N26 within the special research area "Quasi Monte-Carlo Methods and applications" founded by the Austrian Science Fund.

References

1. R.C. Baker, Entire functions and uniform distribution modulo 1. Proc. Lond. Math. Soc. (3) **49**(1), 87–110 (1984)
2. V. Becher, P.A. Heiber, T.A. Slaman, A polynomial-time algorithm for computing absolutely normal numbers. Inf. Comput. **232**, 1–9 (2013)
3. V. Bergelson, E. Lesigne, Van der Corput sets in $\mathbb{Z}^d$. Colloq. Math. **110**(1), 1–49 (2008)
4. V. Bergelson, G. Kolesnik, M. Madritsch, Y. Son, R. Tichy, Uniform distribution of prime powers and sets of recurrence and van der Corput sets in $\mathbb{Z}^k$. Israel J. Math. **201**(2), 729–760 (2014)
5. A. Bertrand-Mathis, Ensembles intersectifs et récurrence de Poincaré. Israel J. Math. **55**(2), 184–198 (1986)
6. M. Boshernitzan, G. Kolesnik, A. Quas, M. Wierdl, Ergodic averaging sequences. J. Anal. Math. **95**, 63–103 (2005)
7. J. Bourgain, Ruzsa's problem on sets of recurrence. Israel J. Math. **59**(2), 150–166 (1987)
8. Y. Bugeaud, *Distribution Modulo One and Diophantine Approximation*. Cambridge Tracts in Mathematics, vol. 193 (Cambridge University Press, Cambridge, 2012)
9. D. Champernowne, The construction of decimals normal in the scale of ten. J. Lond. Math. Soc. **8**, 254–260 (1933) (English)
10. A.H. Copeland, P. Erdős, Note on normal numbers. Bull. Am. Math. Soc. **52**, 857–860 (1946)
11. H. Davenport, P. Erdős, Note on normal decimals. Can. J. Math. **4**, 58–63 (1952)
12. M. Drmota, R.F. Tichy, *Sequences, Discrepancies and Applications*. Lecture Notes in Mathematics, vol. 1651 (Springer, Berlin, 1997)
13. M. Einsiedler, T. Ward, *Ergodic Theory with a View Towards Number Theory*. Graduate Texts in Mathematics, vol. 259 (Springer, Berlin, 2011)
14. H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. J. Anal. Math. **31**, 204–256 (1977)
15. T. Kamae, M. Mendès France, van der Corput's difference theorem. Israel J. Math. **31**(3–4), 335–342 (1978)
16. L. Kuipers, H. Niederreiter, *Uniform Distribution of Sequences*. Pure and Applied Mathematics (Wiley, New York, 1974)
17. M.G. Madritsch, Construction of normal numbers via pseudo-polynomial prime sequences. Acta Arith. **166**(1), 81–100 (2014)
18. M.G. Madritsch, R.F. Tichy, Construction of normal numbers via generalized prime power sequences. J. Integer Seq. **16**(2) (2013). Article 13.2.12, 17
19. M.G. Madritsch, J.M. Thuswaldner, R.F. Tichy, Normality of numbers generated by the values of entire functions. J. Number Theory **128**(5), 1127–1145 (2008)
20. H.L. Montgomery, Ten lectures on the interface between analytic number theory and harmonic analysis, in *CBMS Regional Conference Series in Mathematics*, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994
21. R. Nair, On certain solutions of the Diophantine equation $x - y = p(z)$. Acta Arith. **62**(1), 61–71 (1992)
22. Y. Nakai, I. Shiokawa, A class of normal numbers. Japan. J. Math. (N.S.) **16**(1), 17–29 (1990)
23. Y. Nakai, I. Shiokawa, Discrepancy estimates for a class of normal numbers. Acta Arith. **62**(3), 271–284 (1992)
24. Y. Nakai, I. Shiokawa, Normality of numbers generated by the values of polynomials at primes. Acta Arith. **81**(4), 345–356 (1997)
25. I.Z. Ruzsa, *Connections Between the Uniform Distribution of a Sequence and Its Differences*. Topics in Classical Number Theory, vol. I, II (Budapest, 1981); Colloq. Math. Soc. János Bolyai, vol. 34, (North-Holland, Amsterdam, 1984), pp. 1419–1443
26. A. Sárközy, On difference sets of sequences of integers. I. Acta Math. Acad. Sci. Hung. **31**(1–2), 125–149 (1978)

27. A. Sárközy, On difference sets of sequences of integers. II. Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **21**, 45–53 (1978/1979)
28. A. Sárközy, On difference sets of sequences of integers. III. Acta Math. Acad. Sci. Hung. **31**(3–4), 355–386 (1978)
29. J. Schiffer, Discrepancy of normal numbers. Acta Arith. **47**(2), 175–186 (1986)
30. W. Sierpinski, Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'une tel nombre. Bull. Soc. Math. France **45**, 125–132 (1917)
31. A.M. Turing, A note on normal numbers, in *Collected Works of A.M. Turing*, ed. by J. Britton (North Holland, Amsterdam, 1992), pp. 117–119.
32. P. Walters, *An Introduction to Ergodic Theory*. Graduate Texts in Mathematics, vol. 79 (Springer, Berlin, 1982)

Asymptotics and Equidistribution of Cotangent Sums Associated with the Estermann and Riemann Zeta Functions

Helmut Maier and Michael Th. Rassias

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract The Nyman–Beurling criterion is a well-known approach to the Riemann Hypothesis. Certain integrals over Dirichlet series appearing in this approach can be expressed in terms of cotangent sums. These cotangent sums are also associated with the Estermann zeta function. In this paper improvements as well as further generalizations of asymptotic formulas regarding the relevant cotangent sums are obtained. The main result of this paper is the existence of a unique positive measure μ on $\mathbb{R}$ with respect to which normalized versions of these cotangent sums are equidistributed. We also consider the moments of order $2k$ as a function of k.

Keywords Cotangent sums • Dirichlet series • Equidistribution • Estermann zeta function • Fractional part • Moments • Riemann hypothesis • Riemann zeta function

2010 Mathematics subject classification: Primary 26A12; Secondary 11L03, 11M06

H. Maier
Department of Mathematics, University of Ulm, Helmholtzstrasse 18, 89081 Ulm, Germany
e-mail: helmut.maier@uni-ulm.de

M.Th. Rassias (✉)
Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA

Department of Mathematics, ETH-Zürich, Rämistrasse 101, 8092 Zürich, Switzerland
e-mail: michailrassias@math.princeton.edu; michail.rassias@math.ethz.ch

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_18

1 Introduction

Properties of the Estermann zeta function have been used by Balasubramanian et al. [2] to prove asymptotic formulas for mean-values of the product consisting of the Riemann zeta function and a Dirichlet polynomial. These asymptotic formulas contain cotangent sums which also appear in recent work of Bettin and Conrey [4] on period functions. Very recently, Maier and Rassias in their paper [14] prove asymptotic results and upper bounds for the moments of cotangent sums under consideration. Their main result is the existence of a unique positive measure μ on $\mathbb{R}$ with respect to which these cotangent sums are equidistributed.

2 The Cotangent Sum and Its Applications

In the present paper, we consider the following cotangent sum:

Definition 2.1 *If $r, b \in \mathbb{N}$, $b \geq 2$, $1 \leq r \leq b$ and $(r, b) = 1$, we define*

$$c_0\left(\frac{r}{b}\right) := -\sum_{m=1}^{b-1} \frac{m}{b} \cot\left(\frac{\pi m r}{b}\right) .$$

The function $c_0(r/b)$ is odd and has period 1. Its value is an algebraic number. We first exhibit some relations of the cotangent sums to the Estermann and Riemann zeta functions and connections to the Riemann Hypothesis.

Definition 2.2 *The Estermann zeta function $E\left(s, \frac{r}{b}, \alpha\right)$ is defined by the Dirichlet series*

$$E\left(s, \frac{r}{b}, \alpha\right) = \sum_{n \geq 1} \frac{\sigma_\alpha(n) \exp\left(2\pi i n r/b\right)}{n^s} ,$$

where $Re\, s > Re\, \alpha + 1$, $b \geq 1$, $(r, b) = 1$ and

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha .$$

It can be proved that the Estermann zeta function can be continued analytically to a meromorphic function, on the whole complex plane up to two simple poles $s = 1$ and $s = 1 + \alpha$ if $\alpha \neq 0$ or a double pole at $s = 1$ if $\alpha = 0$ (see [9, 11, 17]).

The Estermann zeta function satisfies the functional equation:

$$E\left(s,\frac{r}{b},\alpha\right)=\frac{1}{\pi}\left(\frac{b}{2\pi}\right)^{1+\alpha-2s}\Gamma(1-s)\Gamma(1+\alpha-s)$$
$$\times\left(\cos\left(\frac{\pi\alpha}{2}\right)E\left(1+\alpha-s,\frac{\overline{r}}{b},\alpha\right)-\cos\left(\pi s-\frac{\pi\alpha}{2}\right)E\left(1+\alpha-s,-\frac{\overline{r}}{b},\alpha\right)\right),$$

where $\overline{r}$ is such that $\overline{r}r\equiv 1 \pmod b$ and $\Gamma(s)$ stands for the Gamma function.

Balasubramanian et al. [2] used properties of $E\left(0,\frac{r}{b},0\right)$ to prove an asymptotic formula for

$$I=\int_0^T\left|\zeta\left(\frac{1}{2}+it\right)\right|^2\left|A\left(\frac{1}{2}+it\right)\right|^2dt\,,$$

where $A(s)$ is a Dirichlet polynomial.

Asymptotics for functions of the form of I have been used for theorems which give a lower bound for the portion of zeros of the Riemann zeta-function $\zeta(s)$ on the critical line (see [12, 13]).

A nice result concerning the value of $E\left(s,\frac{r}{b},\alpha\right)$ at $s=0$ was presented by Ishibashi in [10].

Theorem 2.3 (Ishibashi) *Let $b\geq 2$, $1\leq r\leq b$, $(r,b)=1$, $\alpha\in\mathbb{N}\cup\{0\}$. Then*

(1) If α is even, it holds

$$E\left(0,\frac{r}{b},\alpha\right)=\left(-\frac{i}{2}\right)^{\alpha+1}\sum_{m=1}^{b-1}\frac{m}{b}\cot^{(\alpha)}\left(\frac{\pi mr}{b}\right)+\frac{1}{4}\delta_{\alpha,0}\,,$$

where $\delta_{\alpha,0}$ is the Kronecker delta function.

(2) If α is odd, it holds

$$E\left(0,\frac{r}{b},\alpha\right)=\frac{B_{\alpha+1}}{2(\alpha+1)}\,.$$

If $r=b=1$, one has

$$E(0,1,\alpha)=\frac{(-1)^{\alpha+1}B_{\alpha+1}}{2(\alpha+1)}\,,$$

where B_α denotes the Bernoulli number (see Definition 2.4).

Hence for $b\geq 2$, $1\leq r\leq b$, $(r,b)=1$, we have

$$E\left(0,\frac{r}{b},0\right)=\frac{1}{4}+\frac{i}{2}c_0\left(\frac{r}{b}\right)\,,$$

where $c_0(r/b)$ is the cotangent sum (see Definition 2.1).

The above result gives a relation between the cotangent sum $c_0(r/b)$ and the Estermann zeta function.

The cotangent sum $c_0(r/b)$ can be associated with the so-called Vasyunin sum, which is defined as follows:

$$V\left(\frac{r}{b}\right) := \sum_{m=1}^{b-1} \left\{\frac{mr}{b}\right\} \cot\left(\frac{\pi mr}{b}\right),$$

where $\{u\} = u - \lfloor u \rfloor$, $u \in \mathbb{R}$.

One can prove that (see [3, 4])

$$V\left(\frac{r}{b}\right) = -c_0\left(\frac{\overline{r}}{b}\right),$$

where, as mentioned previously, $\overline{r}$ is such that $\overline{r}r \equiv 1 \pmod{b}$.

The Vasyunin sum [19] is itself associated with the study of the Riemann Hypothesis through the following identity (see [3, 4]):

$$\frac{1}{2\pi(rb)^{1/2}} \int_{-\infty}^{+\infty} \left|\zeta\left(\frac{1}{2}+it\right)\right|^2 \left(\frac{r}{b}\right)^{it} \frac{dt}{\frac{1}{4}+t^2} = \frac{\log 2\pi - \gamma}{2}\left(\frac{1}{r}+\frac{1}{b}\right) + \frac{b-r}{2rb}\log\frac{r}{b} - \frac{\pi}{2rb}\left(V\left(\frac{r}{b}\right)+V\left(\frac{b}{r}\right)\right). \tag{2.1}$$

The only non-explicit function in the right-hand side of (2.1) is the Vasyunin sum.

Formula (2.1) is related to the Nyman–Beurling–Baéz-Duarte–Vasyunin approach to the Riemann Hypothesis (see [1, 3]). The Riemann Hypothesis is true if and only if

$$\lim_{N\to+\infty} d_N = 0,$$

where

$$d_N^2 = \inf_{D_N} \frac{1}{2\pi} \int_{-\infty}^{+\infty} \left|1 - \zeta\left(\frac{1}{2}+it\right) D_N\left(\frac{1}{2}+it\right)\right|^2 \frac{dt}{\frac{1}{4}+t^2}$$

and the infimum is taken over all Dirichlet polynomials

$$D_N(s) = \sum_{n=1}^{N} \frac{a_n}{n^s}.$$

From the above considerations we see that the behavior of $c_0(r/b)$ helps to understand the behavior of $V(r/b)$. From (2.1) we may hope to obtain some

information related to the Nyman–Beurling–Baéz-Duarte–Vasyunin approach to the Riemann Hypothesis.

Definition 2.4 *The m-th Bernoulli number B_m is defined by*

$$B_{2m} = 2\frac{(2m)!}{(2\pi)^{2m}} \sum_{\nu \geq 1} \nu^{-2m}, \quad B_{2m+1} = 0\,,$$

where $m \in \mathbb{N}$. Furthermore, we have $B_{-1} = -1/2$.

3 Main Result

We now discuss the equidistribution of certain normalized cotangent sums with respect to a positive measure, which is also constructed in the following theorem.

Definition 3.1 *For $z \in \mathbb{R}$, let*

$$F(z) = meas\{\alpha \in [0,1] \,:\, g(\alpha) \leq z\},$$

where "meas" denotes the Lebesgue measure,

$$g(\alpha) = \sum_{l=1}^{+\infty} \frac{1 - 2\{l\alpha\}}{l}$$

and

$C_0(\mathbb{R})$=$\{f \in C(\mathbb{R}) : \forall \epsilon > 0, \exists$ *a compact set* $\mathcal{K} \subset \mathbb{R}$, *such that* $|f(x)| < \epsilon, \forall x \notin \mathcal{K}\}$.

Remark The convergence of this series has been investigated by de la Bretèche and Tenenbaum (see [7]). It depends on the partial fraction expansion of the number α.

We now state Theorem 3.2, the main result of our paper. An overview of the basic steps of its proof is provided in Sect. 4. The only fact, whose proof is provided in greater detail, is stated in Lemma 4.8. It implies the continuity of the distribution function of the cotangent sums c_0.

Theorem 3.2

(i) F is a continuous function of z.
(ii) Let A_0, A_1 be fixed constants, such that $1/2 < A_0 < A_1 < 1$. Let also

$$H_k = \int_0^1 \left(\frac{g(x)}{\pi}\right)^{2k} dx,$$

where H_k is a positive constant depending only on k, $k \in \mathbb{N}$.

There is a unique positive measure μ on $\mathbb{R}$ with the following properties:

(a) For $\alpha < \beta \in \mathbb{R}$ we have

$$\mu([\alpha, \beta]) = (A_1 - A_0)(F(\beta) - F(\alpha)).$$

(b)

$$\int x^k d\mu = \begin{cases} (A_1 - A_0)H_{k/2}\,, & \text{for even } k \\ 0\,, & \text{otherwise}\,. \end{cases}$$

(c) For all $f \in C_0(\mathbb{R})$, we have

$$\lim_{b\to+\infty} \frac{1}{\phi(b)} \sum_{\substack{r\,:\,(r,b)=1 \\ A_0 b \le r \le A_1 b}} f\left(\frac{1}{b} c_0\left(\frac{r}{b}\right)\right) = \int f\, d\mu,$$

where $\phi(\cdot)$ denotes the Euler phi-function.

Remark Bruggeman (see [5, 6]) and Vardi (see [18]) have studied the equidistribution of Dedekind sums. In contrast with the work in this paper, they consider an additional averaging over the denominator.

4 Outline of the Proof and Further Results

Rassias [15, 16] proved the following asymptotic formula:

Theorem 4.1 *For $b \ge 2$, $b \in \mathbb{N}$, we have*

$$c_0\left(\frac{1}{b}\right) = \frac{1}{\pi}\, b \log b - \frac{b}{\pi}(\log 2\pi - \gamma) + O(1)\,.$$

In that paper, the fractional parts are expressed in terms of cotangent sums. This method is generalized in the present paper, where some stronger results are being proved.

In [16] also the following improvement of Theorem 4.1 is proved. It is not needed in the proof of Theorem 3.2.

Theorem 4.2 *Let $b, n \in \mathbb{N}$, $b \ge 6N$, with $N = \lfloor n/2 \rfloor + 1$. There exist absolute real constants $A_1, A_2 \ge 1$ and absolute real constants E_l, $l \in \mathbb{N}$ with $|E_l| \le (A_1 l)^{2l}$, such that for each $n \in \mathbb{N}$ we have*

$$c_0\left(\frac{1}{b}\right) = \frac{1}{\pi} b \log b - \frac{b}{\pi}(\log 2\pi - \gamma) - \frac{1}{\pi} + \sum_{l=1}^{n} E_l b^{-l} + R_n^*(b)$$

where

$$|R_n^*(b)| \le (A_2 n)^{4n}\, b^{-(n+1)}.$$

In the following Proposition 4.3, due to the second author (see [16]), a relation is obtained between the cotangent sum c_0 and the modified sum Q. Thus the study of c_0 is reduced to the study of Q, which is crucial. In [16] also Theorem 4.4 is proved.

Proposition 4.3 *For $r, b \in \mathbb{N}$ with $(r, b) = 1$, it holds*

$$c_0\left(\frac{r}{b}\right) = \frac{1}{r}\, c_0\left(\frac{1}{b}\right) - \frac{1}{r} Q\left(\frac{r}{b}\right),$$

where

$$Q\left(\frac{r}{b}\right) = \sum_{m=1}^{b-1} \cot\left(\frac{\pi m r}{b}\right) \left\lfloor \frac{rm}{b} \right\rfloor.$$

Theorem 4.4 *Let $r, b_0 \in \mathbb{N}$ be fixed, with $(b_0, r) = 1$. Let b be a positive integer such that $b \equiv b_0 \pmod r$. Then, there exists a constant $C_1 = C_1(r, b_0)$, with $C_1(1, b_0) = 0$, satisfying*

$$c_0\left(\frac{r}{b}\right) = \frac{1}{\pi r} b \log b - \frac{b}{\pi r}(\log 2\pi - \gamma) + C_1\, b + O(1),$$

for large integer values of b.

We now list other results proven in [16]. In the sequel we shall give a few hints concerning their proofs.

Theorem 4.5 *Let $k \in \mathbb{N}$ be fixed. Let also A_0, A_1 be fixed constants such that $1/2 < A_0 < A_1 < 1$. Then there exist explicit constants $E_k > 0$ and $H_k > 0$, depending only on k, such that*

(a)

$$\sum_{\substack{r:(r,b)=1 \\ A_0 b \le r \le A_1 b}} Q\left(\frac{r}{b}\right)^{2k} = E_k \cdot (A_1^{2k+1} - A_0^{2k+1}) b^{4k} \phi(b)(1 + o(1)), \quad (b \to +\infty).$$

(b)

$$\sum_{\substack{r:(r,b)=1 \\ A_0 b \le r \le A_1 b}} Q\left(\frac{r}{b}\right)^{2k-1} = o\left(b^{4k-2}\phi(b)\right), \quad (b \to +\infty).$$

(c)

$$\sum_{\substack{r:(r,b)=1\\ A_0 b\le r\le A_1 b}} c_0\left(\frac{r}{b}\right)^{2k} = H_k\cdot(A_1-A_0)b^{2k}\phi(b)(1+o(1)),\quad (b\to+\infty).$$

(d)

$$\sum_{\substack{r:(r,b)=1\\ A_0 b\le r\le A_1 b}} c_0\left(\frac{r}{b}\right)^{2k-1} = o\left(b^{2k-1}\phi(b)\right),\quad (b\to+\infty).$$

Applying the method of moments, we deduce detailed information about the distribution of the values of $c_0(r/b)$, where $A_0 b \le r \le A_1 b$ and $b \to +\infty$. In fact, we prove Theorem 3.2.

Finally, we study the convergence of the series

$$\sum_{k\ge 0} H_k x^{2k}$$

and prove the following theorem:

Theorem 4.6 *The series*

$$\sum_{k\ge 0} H_k x^{2k},$$

converges only for $x = 0$.

Another interesting question is whether the series

$$\sum_{k\ge 0} \frac{H_k}{(2k)!} x^{2k},$$

has a positive radius of convergence. This would lead to a simplification in the proof of our equidistribution result, since in this case we could apply the theory of distributions which are determined by their moments. We now give a few hints concerning the proofs of Theorems 4.4 and 4.5.

By Proposition 4.3 we know that

$$c_0\left(\frac{r}{b}\right) = \frac{1}{r}c_0\left(\frac{1}{b}\right) - \frac{1}{r}Q\left(\frac{r}{b}\right),$$

where

$$Q\left(\frac{r}{b}\right) = \sum_{m=1}^{b-1} \cot\left(\frac{\pi m r}{b}\right)\left\lfloor \frac{rm}{b}\right\rfloor .$$

We partition the range of the above summation into intervals on which the term $\lfloor rm/b \rfloor$ assumes a constant value j:

$$Q\left(\frac{r}{b}\right) = \sum_{j=0}^{r-1} j \sum_{j \le \lfloor \frac{rm}{b} \rfloor < j+1} \cot\left(\frac{\pi m r}{b}\right)$$

and define

$$S_j = \{rm \,:\, bj \le rm < b(j+1), m \in \mathbb{Z}\}.$$

We write

$$S_j = \{bj + s_j, bj + s_j + r, \ldots, bj + s_j + d_j r\},$$

where $d_j \in \{0, 1\}$ and introduce $s = s_j$ as a new variable of summation.

The relation between j and s_j is given by

$$s_j \equiv -bj (\mathrm{mod} r)$$

and thus for a given value $s_j = s$ we can find j by

$$\frac{j}{r} = \left\{-\frac{sb^*}{r}\right\},$$

where b^* is defined by

$$bb^* \equiv 1 (\mathrm{mod} r),\ 1 \le b^* \le r - 1.$$

Since $\cot(\pi x)$ has a pole of first order at $x = 0$, the sum $Q(r/b)$ is dominated by small values of s. The substitution

$$\alpha = \alpha(r, b) = \frac{b^*}{r}$$

and the asymptotics

$$\cot(\pi x) \sim \frac{1}{\pi x}$$

lead to the approximation of $Q(r/b)$ by

$$\frac{br}{\pi} g(\alpha).$$

For the proof of Theorem 1.5 of [14], the crucial property is the continuity of the function $F(z)$, where

$$F(z) = \text{meas}\{\alpha \in [0,1] \ : \ g(\alpha) \le z\}.$$

We shall give a proof of this fact shortly. The proof of Theorem 4.6 is obtained by studying the contribution of the interval

$$I(k) = [e^{-2k-1}, e^{-2k}]$$

to the moment

$$H_k = \int_0^1 \left(\frac{g(x)}{\pi}\right)^{2k} dx\,.$$

Definition 4.7 *A distribution function G is a monotonically increasing function*

$$G : \mathbb{R} \to [0,1].$$

The characteristic function ψ of G is defined by the following Stieltjes integral:

$$\psi(t) = \int_{-\infty}^{+\infty} e^{itu} dG(u).$$

(cf. [8, p.27])

Lemma 4.8 *The distribution function G is continuous if and only if the characteristic function ψ satisfies*

$$\liminf_{T\to+\infty} \frac{1}{2T} \int_{-T}^{T} |\psi(t)|^2 dt = 0.$$

Proof See [8, p. 48, Lemma 1.23].

Definition 4.9 *Let $t \ge 1$. We set*

$$K = K(t) = \lfloor t^{9/10} \rfloor,\ L = L(t) = \lfloor t^{11/10} \rfloor,\ R = R(t) = \lfloor t^{9/5} \rfloor$$

and

$$g(\alpha, K) = -2 \sum_{l \le K} \frac{B^*(l\alpha)}{l},\ \ h(\alpha) = -2 \sum_{l > K} \frac{B^*(l\alpha)}{l},$$

where $B^*(u) = u - \lfloor u \rfloor - 1/2$, $u \in \mathbb{R}$.

Assume that (α_i) *with* $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_R = 1$ *is a partition of* $[0, 1]$ *with the following properties:*

$$\frac{1}{2}R^{-1} \leq \alpha_{i+1} - \alpha_i \leq 2R^{-1}$$

and $g(\alpha, K)$ *is continuous at* $\alpha = \alpha_i$ *for* $0 < i < R$.

We now make preparations for an application of Lemma 4.8 with $G = F$, and

$$\psi(t) = \Phi(t) := \int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha.$$

Lemma 4.10 *The function* $h(\alpha)$ *has a Fourier expansion*

$$h(\alpha) = \sum_{n>K} c(n) \sin(2\pi n\alpha),$$

with

$$|c(n)| \leq \frac{2\tau(n)}{\pi n},$$

where τ *stands for the divisor function.*

Proof From the Fourier expansion

$$B^*(u) = \frac{i}{2\pi} \sum_{\substack{n=-\infty \\ n\neq 0}}^{+\infty} \frac{e(nu)}{n},$$

we obtain

$$h(\alpha) = -\frac{i}{\pi} \sum_{l>K} \frac{1}{l} \sum_{\substack{m=-\infty \\ m\neq 0}}^{+\infty} \frac{e(lm\alpha)}{m} = \sum_{|n|>K} d(n)e(n\alpha)$$

with

$$d(n) = -\frac{i}{\pi n} \left|\{(l, m) \ : \ lm = n, \ l > K\}\right|.$$

We have

$$h(\alpha) = \sum_{n>K} d(n) \left(e(n\alpha) - e(-n\alpha)\right) = 2i \sum_{n>K} d(n) \sin(2\pi n\alpha),$$

which completes the proof of the lemma.

Definition 4.11 *We set*

$$h_1(\alpha) := \sum_{K<n\le L} c(n)\sin(2\pi n\alpha)$$

and

$$h_2(\alpha) := \sum_{n>L} c(n)\sin(2\pi n\alpha).$$

Lemma 4.12 *We have*

$$\int_0^1 \left(e\left(\frac{t}{2\pi}\left(g(\alpha,K)+h_1(\alpha)\right)\right) - e\left(\frac{tg(\alpha)}{2\pi}\right)\right) d\alpha = O\left(t^{-1/100}\right).$$

Proof By Parseval's identity, it follows that for every $\epsilon > 0$ it holds

$$\int_0^1 h_2(\alpha)^2 d\alpha = \sum_{n>L} c(n)^2 \ll L^{-(1-2\epsilon)},$$

because of the estimate

$$c(n) \ll n^{-1+\epsilon}.$$

Thus, for all $\alpha \in [0,1]$ not belonging to an exceptional set $\mathcal{E}$ with

$$\text{meas}(\mathcal{E}) = O\left(t^{-1/100}\right),$$

we have

$$h_2(\alpha) = O\left(t^{-1-1/100}\right)$$

and therefore

$$\left| e\left(\frac{th_2(\alpha)}{2\pi}\right) - 1\right| = O\left(t^{-1/100}\right)$$

by the Taylor expansion of the exponential function.

Hence,

$$\left|\int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha - \int_0^1 e\left(\frac{t}{2\pi}(g(\alpha,K)+h_1(\alpha))\right) d\alpha\right|$$
$$\le \int_0^1 \left| e\left(\frac{t(g(\alpha,K)+h_1(\alpha))}{2\pi}\right)\right| \left| e\left(\frac{th_2(\alpha)}{2\pi}\right) - 1\right| d\alpha$$

$$\leq \int_{\mathcal{E}} 2\, d\alpha + \int_{[0,1]\setminus\mathcal{E}} \left| e\left(\frac{th_2(\alpha)}{2\pi}\right) - 1 \right| d\alpha$$
$$= O\left(t^{-1/100}\right).$$

Lemma 4.13 *There exists a set $I \subseteq \{1, \ldots, R\}$ of non-negative integers, such that*

$$\sum_{i\in I} (\alpha_{i+1} - \alpha_i) = O\left(t^{-1/100}\right)$$

and for $i \notin I$, $\alpha \in [\alpha_i, \alpha_{i+1}]$ we have

$$|h_1(\alpha) - h_1(\alpha_i)| \leq t^{-(1+1/100)}.$$

Proof We have

$$\frac{d}{d\alpha} h_1(\alpha) = \sum_{K<n\leq L} 2\pi n c(n) \cos(2\pi n\alpha)$$

and

$$\frac{d^2}{d\alpha^2} h_1(\alpha) = -\sum_{K<n\leq L} 4\pi^2 n^2 c(n) \sin(2\pi n\alpha).$$

By Parseval's identity, for every $\epsilon > 0$ we get

$$\int_0^1 \left| \frac{d}{d\alpha} h_1(\alpha) \right|^2 d\alpha = O\left(L^{1+2\epsilon}\right)$$

and by the Cauchy–Schwarz inequality, it follows that

$$\int_0^1 \left| \frac{d}{d\alpha} h_1(\alpha) \right| d\alpha = O\left(L^{1/2+\epsilon}\right). \tag{4.1}$$

We now define the set I as the set of all subscripts i for which the closed interval $[\alpha_i, \alpha_{i+1}]$ contains an α with

$$|h_1(\alpha) - h_1(\alpha_i)| > t^{-(1+1/100)}.$$

Since

$$h_1(\alpha) = h_1(\alpha_i) + \int_{\alpha_i}^{\alpha} \frac{d}{d\beta} h_1(\beta) d\beta \tag{4.2}$$

and

$$|\alpha - \alpha_i| = O\left(t^{-9/5}\right),$$

it follows that for $i \in I$ there must exist $\beta \in (\alpha_i, \alpha_{i+1})$ with

$$\left|\frac{d}{d\beta}h_1(\beta)\right| \geq t^{3/5}.$$

Because of the estimation of the Fourier coefficients of $\frac{d^2}{d\alpha^2}h_1(\alpha)$, we obtain

$$\left|\frac{d^2}{d\alpha^2}h_1(\alpha)\right| = O\left(L^{2+\epsilon}\right).$$

Analogously to (4.2) we obtain that

$$\left|\frac{d}{d\alpha}h_1(\alpha)\right| \geq \frac{1}{2}t^{3/5},$$

for every $\alpha \in [\alpha_i, \alpha_{i+1}]$ and therefore

$$\int_{a_i}^{a_{i+1}} \left|\frac{d}{d\alpha}h_1(\alpha)\right| d\alpha \geq \frac{1}{2}t^{3/5}(\alpha_{i+1} - \alpha_i).$$

From (4.1) we obtain that the measure of the union of the closed intervals $[\alpha_i, \alpha_{i+1}]$ with $i \in I$ is $O(t^{-1/100})$, which concludes the proof of the lemma.

Lemma 4.14 *We have*

$$\lim_{t\to+\infty} \Phi(t) = \lim_{t\to-\infty} \Phi(t) = 0.$$

Proof We shall prove the result only for $t \to +\infty$, since the proof of the part when $t \to -\infty$ is analogous.

By Lemma 4.12, we have

$$\Phi(t) = \int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha = \int_0^1 e\left(\frac{t}{2\pi}(g(\alpha, K) + h_2(\alpha))\right) + O\left(t^{-1/100}\right)$$

and thus

$$\Phi(t) = \int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha = \sum_{\substack{i=0 \\ i\notin I}}^{R} e\left(\frac{th_1(\alpha_i)}{2\pi}\right) \int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) d\alpha$$
$$+ \sum_{\substack{i=0 \\ i\notin I}}^{R} \int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) \left(e\left(\frac{th_1(\alpha)}{2\pi}\right) - e\left(\frac{th_1(\alpha_i)}{2\pi}\right)\right) d\alpha$$
$$+ O\left(\sum_{i\in I}(\alpha_{i+1}-\alpha_i)\right) + O\left(t^{-1/100}\right).$$

From Lemma 4.13 we get

$$\Phi(t)= \int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha= \sum_{\substack{i=0 \\ i\notin I}}^{R} e\left(\frac{th_1(\alpha_i)}{2\pi}\right) \int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) d\alpha+O\left(t^{-1/100}\right). \tag{4.3}$$

We now estimate

$$\int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) d\alpha,$$

for $i \notin I$. Let $J_i - 1$ be the number of discontinuities of the function $g(\alpha, K)$ in the interval $[\alpha_i, \alpha_{i+1}]$. Let $\beta_{i,0} = \alpha_i$, $\beta_{i,J_i} = \alpha_{i+1}$ and let the discontinuities of $g(\alpha, K)$ in $[\alpha_i, \alpha_{i+1}]$ occur at the points $\beta_{i,1} < \beta_{i,2} < \cdots < \beta_{i,J_i-1}$.

In the intervals $[\beta_{i,r}\ ,\ \beta_{i,r+1}]$ the function $g(\alpha, K)$ is a linear function, that is

$$g(\alpha, K) = d_r - 2K\alpha,$$

where $d_r \in \mathbb{R}$. Therefore,

$$\left|\int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) d\alpha\right| \le \sum_{r=0}^{J_i} \left|\int_{\beta_{i,r}}^{\beta_{i,r+1}} e\left(\frac{tg(\alpha,K)}{2\pi}\right) d\alpha\right|$$
$$\le \sum_{r=0}^{J_i} \left|\int_{\beta_{i,r}}^{\beta_{i,r+1}} e\left(-\frac{tK\alpha}{\pi}\right) d\alpha\right|$$
$$= O\left(J_i(tK)^{-1}\right). \tag{4.4}$$

From (4.3) and (4.4), we get

$$\int_0^1 e\left(\frac{tg(\alpha)}{2\pi}\right) d\alpha \le \sum_{\substack{i=0 \\ i\notin I}}^{R} \left| \int_{\alpha_i}^{\alpha_{i+1}} e\left(\frac{tg(\alpha, K)}{2\pi}\right) d\alpha \right| + O\left(t^{-1/100}\right)$$

$$= O\left((tK)^{-1} \sum_{\substack{i=0 \\ i\notin I}}^{R} J_i \right) + O\left(t^{-1/100}\right).$$

The number of discontinuities of $g(\alpha, K)$ is $O(K^2)$, since each of the K terms

$$\frac{B^*(l\alpha)}{l}$$

has $O(K)$ discontinuities in the interval $[0, 1]$. We thus have

$$\sum_{i=0}^{R} J_i = O(K^2).$$

Then

$$\Phi(t) = O\left(t^{-1/100}\right).$$

Therefore

$$\lim_{t\to+\infty} \Phi(t) = 0.$$

Similarly, we obtain

$$\lim_{t\to-\infty} \Phi(t) = 0,$$

which completes the proof of the lemma.

Lemma 4.15 *F is a continuous function of z.*

Proof This follows from Lemmas 4.8 and 4.14.

Thus, part (i) of Theorem 3.2 is now proved.

Acknowledgements We express our thanks to the referee for providing valuable remarks.

References

1. B. Bagchi, On Nyman, Beurling and Baez-Duarte's Hilbert space reformulation of the Riemann hypothesis. Proc. Indian Acad. Sci. Math. **116**(2), 137–146 (2006)
2. R. Balasubramanian, J.B. Conrey, D.R. Heath-Brown, Asymptotic mean square of the product of the Riemann zeta-function and a Dirichlet polynomial. J. Reine Angew. Math. **357**, 161–181 (1985)
3. S. Bettin, A generalization of Rademacher's reciprocity law. Acta Arith. **159**(4), 363–374 (2013)
4. S. Bettin, B. Conrey, Period functions and cotangent sums. Algebra Number Theory **7**(1), 215–242 (2013)
5. R.W. Bruggeman, Eisenstein series and the distribution of Dedekind sums. Math. Z. **202**, 181–198 (1989)
6. R.W. Bruggeman, Dedekind sums and Fourier coefficients of modular forms. J. Number Theory **36**, 289–321 (1990)
7. R. de la Bretèche, G. Tenenbaum, Séries trigonométriques à coefficients arithmétiques. J. Anal. Math. **92**, 1–79 (2004)
8. P.D.T.A. Elliott, *Probabilistic Number Theory I: Mean-Value Theorems* (Springer, New York, 1979)
9. T. Estermann, On the representation of a number as the sum of two products. Proc. Lond. Math. Soc. **31**(2), 123–133 (1930)
10. M. Ishibashi, The value of the Estermann zeta function at $s = 0$. Acta Arith. **73**(4), 357–361 (1995)
11. M. Ishibashi, $\mathbb{Q}$-linear relations of special values of the Estermann zeta function. Acta Arith. **86**(3), 239–244 (1998)
12. H. Iwaniec, On the mean values for Dirichlet's polynomials and the Riemann zeta function. J. Lond. Math. Soc. **22**(2), 39–45 (1980)
13. H. Iwaniec, E. Kowalski, *Analytic Number Theory*. American Mathematical Society Colloquium, vol. 53 (American Mathematical Society, Providence, RI, 2004)
14. H. Maier, M.Th. Rassias, Generalizations of a cotangent sum associated to the Estermann zeta function. Commun. Contemp. Math. **18**(1), 89 pp. (2016). doi:10.1142/S0219199715500789
15. M.Th. Rassias, On a cotangent sum related to zeros of the Estermann zeta function. Appl. Math. Comput. **240**, 161–167 (2014)
16. M.Th. Rassias, Analytic investigation of cotangent sums related to the Riemann zeta function. Doctoral dissertation, ETH-Zürich, Switzerland, 2014
17. R. Šleževičiene, J. Steuding, On the zeros of the Estermann zeta-function. Integr. Transf. Spec. Funct. **13**, 363–371 (2002)
18. I. Vardi, Dedekind sums have a limiting distribution. Int. Math. Res. Not. **1**, 1–12 (1993)
19. V.I. Vasyunin, On a biorthogonal system associated with the Riemann hypothesis. Algebra i Analiz **7**(3), 118–135 (1995) (in Russian); English translation in St. Petersburg Math. J. **7**(3), 405–419 (1996)

A Turán-Kubilius Inequality on Mappings of a Finite Set

Eugenijus Manstavičius

Zur Erinnerung an Professor Wolfgang Schwarz

Abstract Similarly as in number theory one may define the notion of an additive function in the set of all mappings of a finite set into itself. If a mapping is sampled uniformly at random, the function becomes a sum of dependent random variables. Estimation of its variance via the sum of variances of the summands is a non-trivial problem. We give an answer analogously to the Turán-Kubilius inequality, well known in probabilistic number theory.

Keywords Additive function • Assembly • Random mapping • Second moment • Turán-Kubilius inequality

2010 Mathematics subject classification: Primary 60C05; Secondary 05A15, 11N37

1 Introduction and Results

The present note concerns random mapping statistics which share many analogies with probabilistic number theory, one of the favourite research fields of Professor Wolfgang Schwarz. During frequent visits to the Goethe University, the author felt the host's interest and encouragement to study a theory of functions defined on decomposable combinatorial structures. It was not a coincidence, that our paper [9] dedicated to his 70th birthday discussed an analytic approach to explore mean values of multiplicative functions defined on mappings of a finite set into itself, and consequently, to prove limit theorems on value distribution of additive ones. Here we are concerned with the same object but the main target is to prove an analogue of

E. Manstavičius (✉)
Faculty of Mathematics and Informatics, Vilnius University, Naugarduko str. 24, LT-03225 Vilnius, Lithuania
e-mail: eugenijus.manstavicius@mif.vu.lt

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_19

the Turán-Kubilius inequality (see [7], Lemma 3.1) for the second central moment. A historical survey of the results for these mappings can be found in [9] and the references therein.

Let us introduce some notation. By $\mathbf{T}_N$ we denote the set of all mappings φ from the set $\{1,\dots,N\}$ into itself. A mapping φ can also be understood as a labelled directed graph G_φ on N vertices which we call a *functional digraph*. In G_φ, an edge from i to j exists if and only if $\varphi(i) = j$. Many properties of φ can be expressed via the component vector $\bar{k}(\varphi) = (k_1(\varphi),\dots,k_N(\varphi))$, where $k_j(\varphi)$ is the number of connected components of order (number of vertices) j in G_φ. By definition,

$$1k_1(\varphi) + \cdots + Nk_N(\varphi) = N. \tag{1.1}$$

Let $\nu_N(\dots) = N^{-N}|\{\varphi \in \mathbf{T}_N\colon \dots\}|$ be the uniform probability measure on $\mathbf{T}_N$. Observe that relation (1.1) makes the variables $k_j(\varphi)$, $1 \le j \le N$, dependent with respect to ν_N. Given a real two-dimensional array $\{h_j(k)\}$, where $j \ge 1$ and $k \ge 0$, such that $h_j(0) \equiv 0$, we define an *additive function* $h(\varphi)$ in $\mathbf{T}_N$ by setting

$$h(\varphi) = \sum_{j=1}^{N} h_j(k_j(\varphi)). \tag{1.2}$$

If $h_j(s) = sa_j$ with some a_j for each $j, s \ge 1$, then the function $h(\varphi)$ is called *completely additive*, and equals just a linear combination of $k_j(\varphi)$. The number of components $w(\varphi) := k_1(\varphi)+\cdots+k_N(\varphi)$ is the simplest example of such a function. Changing the sum in (1.2) to the product, in a similar manner, we obtain the notion of a *multiplicative* function in $\mathbf{T}_N$.

Denote by m_j the number of connected functional digraphs of order $j \ge 1$. It is known [1, 4] that

$$m_j = (j-1)!\sum_{s=0}^{j-1}\frac{j^s}{s!} =: j!\mathrm{e}^j\lambda_j, \qquad \left|\lambda_j - \frac{1}{2j}\right| \le \frac{8}{j^{3/2}} \tag{1.3}$$

if $j \ge 1$. The last inequality was proved by J.C. Hansen [5]. Because of (1.3), the class of mappings of all orders $\mathscr{T} := \cup_{N\ge 0}\mathbf{T}_N$, where $\mathbf{T}_0 = \{\emptyset\}$, is *logarithmic* (see [1]); therefore, many general results obtained for this class (see [1]) or its generalization (see [11]) are at our disposal. Let r, $1 \le r \le N$, be a parameter and write $\bar{k}_r(\varphi) := (k_1(\varphi),\dots,k_r(\varphi))$ for a shortened component vector. If ξ_j, $1 \le j \le r$, are independent Poisson random variables (r.vs) defined on some probability space $(\Omega, \mathscr{F}, P)$, $\mathbf{E}\xi_j = \lambda_j$ and $\bar{\xi}_r := (\xi_1,\dots,\xi_r)$, then we have [1, 11] the following total variation distance estimate

$$\sum_{\bar{s}_r\in\mathbf{N}_0^r}\left|\nu_n\big(\bar{k}_r(\varphi) = \bar{s}_r\big) - P\big(\bar{\xi}_r = \bar{s}_r\big)\right| \ll \Big(\frac{r}{N}\Big)^c, \tag{1.4}$$

where $c > 0$ is an absolute constant. Here and afterwards $\ll$ stands for the symbol $O(\cdot)$ with an absolute constant in it and $X \asymp Y$ means that $X \ll Y$ and $Y \ll X$. So, the value distribution problems concerning the truncated additive function defined only via $\bar{k}_r(\varphi)$ if $r = o(N)$ as $N \to \infty$, can be easily transferred to probability theory. To estimate the influence of the remaining part of an additive function defined via $k_j(\varphi)$, $r < j \le N$, one can use the author's inequality (see [8], Lemma 6) for the tail probability

$$\nu_N\big(|h(\varphi) - a| \ge u\big) \ll P^{1/2}\left(\left|\sum_{j\le N} h_j(\xi_j) - a\right| \ge u/3\right) + \frac{1}{\sqrt{N}}, \quad a \in \mathbf{R},\ u \in \mathbf{R}_+.$$

Moment estimates would be very useful at this stage. Unfortunately, we do not have them so far. In contrast, moments of an additive function defined on permutations have been intensively studied (see [10, 12] and the references therein). Partly filling up the gap, in the present note we will analyse the variance

$$\mathbf{V}_N h(\varphi) := N^{-N} \sum_{\varphi\in\mathbf{T}_N} \big(h(\varphi) - \mathbf{E}_n h(\varphi)\big)^2,$$

where $\mathbf{E}_N$ denote the expectation with respect to ν_N.

It is worth starting with a few known identities which can be deduced using the exponential generating series

$$Z(z) := 1 + \sum_{N=1}^{\infty} \frac{N^N}{N!} z^N = \exp\left\{\sum_{j=1}^{\infty} \frac{m_j}{j!} z^j\right\}$$

corresponding to the class $\mathscr{T}$. Firstly, observe that

$$N^N = N! \sum_{\ell(\bar{s})=N} \prod_{j\le N} \Big(\frac{m_j}{j!}\Big)^{s_j} \frac{1}{s_j!}.$$

Secondly,

$$\nu_N\big(\bar{k}(\varphi) = \bar{s}\big) = \frac{1}{Q(N)} \prod_{j\le N} \Big(\frac{m_j}{j!}\Big)^{s_j} \frac{1}{s_j!} \tag{1.5}$$

for arbitrary vector $\bar{s} \in \mathbf{N}_0^N$ satisfying $\ell(\bar{s}) = N$, where

$$Q(N) := \frac{N^N}{N!} = \frac{\mathrm{e}^N}{\sqrt{2\pi N}}\Big(1 + O\Big(\frac{1}{N}\Big)\Big) \tag{1.6}$$

by Stirling's formula. This gives the rough estimate

$$\frac{\mathrm{e}^j Q(N-j)}{Q(N)} \asymp \Big(1-\frac{j}{N+1}\Big)^{-1/2}, \quad 1 \le j \le N, \tag{1.7}$$

which we will frequently apply in the sequel.

Formula (1.5) defines the distribution of the component vector supported in the region $\ell^{-1}(N)$. Its applications provide formulae for the factorial moments of $k_j(\varphi)$. Set $Q(0) = 1$, $(x)_0 = 1$, and $(x)_r = x(x-1)\cdots(x-r+1)$ if $r \in \mathbf{N}$. We have [1]

$$\mathbf{E}_N\big(k_j(\varphi)\big)_r = \frac{Q(N-jr)}{Q(N)}\Big(\frac{m_j}{j!}\Big)^r \tag{1.8}$$

provided that $jr \le N$ and $\mathbf{E}_N\big(k_j(\varphi)\big)_r = 0$ otherwise. Moreover,

$$\mathbf{E}_N\big(k_j(\varphi)\big)_r\big(k_i(\varphi)\big)_l = \frac{Q(N-jr-il)}{Q(N)}\Big(\frac{m_j}{j!}\Big)^r\Big(\frac{m_i}{i!}\Big)^l, \tag{1.9}$$

provided that $i \ne j$ and $jr + il \le N$ and $\mathbf{E}_N\big(k_j(\varphi)\big)_r\big(k_i(\varphi)\big)_l = 0$ if $i \ne j$ and $jr + il > N$. By (1.6),

$$\mathbf{E}_N\big(k_j(\varphi)\big)_r \sim \lambda_j^r, \qquad \mathbf{E}_N\big(k_j(\varphi)\big)_r\big(k_i(\varphi)\big)_l \sim \lambda_j^r\lambda_i^l$$

provided that i, j, r and l are fixed natural numbers and $N \to \infty$. This, in addition to (1.4), shows asymptotic closeness of $k_j(\varphi)$ to the Poisson r.v. ξ_j. Finally, we recall that the stochastic behaviour of various statistics defined on random mappings is similar to that defined on random permutations sampled according to the Ewens probability with parameter $\theta = 1/2$. Therefore the approach applied in paper [12], exploring in particular this case of permutations, plays an important role. Here, we must also acknowledge the influence of the number-theoretical paper [2].

For the sake of simplicity, our first theorem is stated only for a completely additive function defined via $h_j(s) = sa_j$ with arbitrary $a_j \in \mathbf{R}$, where $j \le n$ and $s \ge 0$. Define

$$B^2(N) := \sum_{j\le N}\frac{a_j^2\mathrm{e}^j Q(N-j)\lambda_j}{Q(N)} \ll \sum_{j\le N}\frac{a_j^2}{j}\Big(1-\frac{j}{N+1}\Big)^{-1/2}.$$

The last estimate follows from (1.3) and (1.7). To motivate the use of $B(N)$ we include the following estimate.

Proposition If

$$R(N) := \sum_{j\le N} \left| \mathbf{V}_N\big(a_j k_j(\varphi)\big) - \frac{a_j^2 \mathrm{e}^j Q(N-j)\lambda_j}{Q(N)} \right|,$$

then $R(N) \ll B^2(N)/\sqrt{N}$.

Theorem 1.1 *For an arbitrary completely additive function and $N \ge 1$, we have*

$$\mathbf{V}_N h(\sigma) \ll B^2(N). \tag{1.10}$$

In the general case, it is natural to use instead of $B^2(N)$ the quantity

$$D^2(N) := \sum_{jk\le N} \frac{h_j^2(k)\lambda_j^k}{k!} \frac{\mathrm{e}^{jk} Q(N-jk)}{Q(N)} \ll \sum_{jk\le N} \frac{h_j^2(k)}{j^k k!} \Big(1 - \frac{jk}{N+1}\Big)^{-1/2}.$$

We introduce the Mth coefficient of the product of two power series by

$$Q^{(j)}(M) := [z^M] Z(z) \exp\Big\{ - \frac{m_j z^j}{j!} \Big\} = \sum_{\substack{\ell(\bar{s})=M \\ s_j=0}} \prod_{i\le M} \Big(\frac{m_i}{i!}\Big)^{s_i} \frac{1}{s_i!}$$

provided $1 \le j \le M \le N$ and $Q^{(j)}(M) := Q(M)$ if $j > M$.

Theorem 1.2 *For an arbitrary real additive function given in* (1.2) *and all $N \ge 1$, we have*

$$\mathbf{E}_n h(\varphi) = \sum_{jk\le N} \frac{h_j(k)\lambda_j^k}{k!} \frac{\mathrm{e}^{jk} Q^{(j)}(N-jk)}{Q(N)}. \tag{1.11}$$

and

$$\mathbf{V}_N h(\varphi) \ll D^2(N). \tag{1.12}$$

The best constant in inequality (1.10), or in (1.12), is the maximal eigenvalue of the involved symmetric matrix. We guess that its numerical estimate is $5/3 + o(1)$ as $N \to \infty$. Following P.D.T.A. Elliott [3], one can find a corresponding dual inequality for either (1.10) or (1.12). Adopting the well-known Rényi's approach proposed in number theory, one can present a simpler proof of Theorem 2 in [9] by establishing an analogue of Delange's theorem for multiplicative number theoretical functions. The list of possible applications of our inequalities could be continued further. Their proofs are presented in the next section.

2 Proofs

Proof of the Proposition We deduce from (1.8) and (1.9) that

$$\mathbf{E}_N k_j(\varphi) = \frac{\mathrm{e}^j Q(N-j)\lambda_j}{Q(N)}, \quad j \le N; \tag{2.1}$$

$$\begin{aligned}\mathbf{E}_N k_j^2(\varphi) &= \mathbf{E}_N k_j(\varphi) + \mathbf{1}\{j \le N/2\}\mathbf{E}_N\big(k_j(\varphi)\big)_2 \\ &= \frac{\mathrm{e}^j Q(N-j)\lambda_j}{Q(N)} + \mathbf{1}\{j \le N/2\}\frac{\mathrm{e}^{2j} Q(N-2j)\lambda_j^2}{Q(N)}\end{aligned} \tag{2.2}$$

and

$$\begin{aligned}\mathbf{V}_N k_j(\varphi) - \frac{\mathrm{e}^j Q(N-j)\lambda_j}{Q(N)} &= \mathbf{1}\{j \le N/2\}\frac{\mathrm{e}^{2j} Q(N-2j)\lambda_j^2}{Q(N)} \\ &\quad - \frac{\mathrm{e}^{2j} Q^2(N-j)\lambda_j^2}{Q^2(N)}.\end{aligned}$$

Hence

$$\begin{aligned}R(N) &= \sum_{j \le N/2} a_j^2 \left| \frac{\mathrm{e}^{2j} Q(N-2j)}{Q(N)} - \frac{\mathrm{e}^{2j} Q^2(N-j)}{Q^2(N)} \right| \lambda_j^2 \\ &\quad + \sum_{N/2 < j \le N} a_j^2 \frac{\mathrm{e}^{2j} Q^2(N-j)}{Q^2(N)} \lambda_j^2.\end{aligned}$$

By virtue of (1.7), the last sum in $R(N)$ is majorised by

$$\begin{aligned}&N^{-1} \sum_{N/2 < j \le N} \frac{a_j^2}{j} \frac{\mathrm{e}^j Q(N-j)}{Q(N)} \Big(1 - \frac{j}{N+1}\Big)^{-1/2} \\ &\ll N^{-1/2} \sum_{N/2 < j \le N} \frac{a_j^2}{j} \frac{\mathrm{e}^j Q(N-j)}{Q(N)} \ll N^{-1/2} B^2(N).\end{aligned}$$

The same argument applies and the estimate holds for the partial sum in $R(N)$ over $N/4 < j \le N/2$. Finally, combining $(1-x)^{-1/2} = 1 + x/2 + O(x^2)$ where $0 \le x \le 1/2$ with the asymptotical formula (1.6), we obtain

$$\sum_{j \le N/4} \frac{a_j^2 \lambda_j}{j} \left| \frac{\mathrm{e}^{2j} Q(N-2j)}{Q(N)} - \frac{\mathrm{e}^{2j} Q^2(N-j)}{Q^2(N)} \right|$$

$$\ll \sum_{j\le N/4} \frac{a_j^2\lambda_j}{j}\left|\left(1-\frac{2j}{N}\right)^{-1/2}-\left(1-\frac{j}{N}\right)^{-1}+\frac{1}{N}\right|$$

$$\ll N^{-1}\sum_{j\le N/4} a_j^2\lambda_j \ll N^{-1}B^2(N).$$

Collecting the estimates for the partial sums we furnish the proof of the proposition.

Proof of Theorem 1.1 Seeking upper estimates we may deal with $a_j \ge 0$ and $j \le N$ only, and later combine the results for positive and negative parts of $h(\sigma)$ with the inequality $(a+b)^2 \le 2a^2+2b^2$, where $a, b \in \mathbf{R}$. Let us calculate the moments of $h(\varphi)$ defined via nonnegative a_j. We deduce from (1.9), (2.1) and (2.2) that

$$\mathbf{E}_N h(\varphi) = \sum_{j\le N} a_j\lambda_j \frac{\mathrm{e}^j Q(N-j)}{Q(N)},$$

and

$$\mathbf{E}_N h^2(\varphi) = B^2(N) + \sum_{i+j\le N} a_i a_j \lambda_i\lambda_j \frac{\mathrm{e}^{i+j}Q(N-i-j)}{Q(N)}.$$

Hence

$$\mathbf{V}_N h(\varphi) = \mathbf{E}_N h^2(\varphi) - \big(\mathbf{E}_N h(\varphi)\big)^2$$

$$= B^2(N) - \sum_{\substack{i,j\le N\\ i+j>N}} a_i a_j \lambda_i\lambda_j \frac{\mathrm{e}^{i+j}Q(N-i)Q(N-j)}{Q^2(N)}$$

$$+ \sum_{i+j\le N} a_i a_j\lambda_i\lambda_j \mathrm{e}^{i+j}\left(\frac{Q(N-i-j)}{Q(N)} - \frac{Q(N-i)Q(N-j)}{Q^2(N)}\right). \tag{2.3}$$

We now omit the non-positive terms on the right-hand side of (2.3) to obtain

$$\mathbf{V}_N h(\varphi) \le B^2(N)$$

$$+ \sum_{i+j\le N} a_i a_j\lambda_i\lambda_j \mathrm{e}^{i+j}\left(\frac{Q(N-i-j)}{Q(N)} - \frac{Q(N-i)Q(N-j)}{Q^2(N)}\right)^+.$$

Here x^+ denotes the positive part of $x \in \mathbf{R}$. The inequality $ab \le (a^2+b^2)/2$ for $a, b \in \mathbf{R}_+$ implies the further relation

$$\mathbf{V}_N h(\varphi) \le B^2(N) + \sum_{j\le N} a_j^2 \lambda_j \mathrm{e}^j \sum_{i\le N-j} \lambda_i \mathrm{e}^i \Big(\frac{Q(N-i-j)}{Q(N)} - \frac{Q(N-i)Q(N-j)}{Q^2(N)} \Big)^+.$$

We now see that an inequality

$$\begin{aligned} \Delta(M) &:= \Big(\sum_{i\le M/2} + \sum_{M/2<i\le M} \Big) \frac{\mathrm{e}^i}{i} \Big(Q(N)Q(M-i) - Q(N-i)Q(M) \Big)^+ \\ &=: \Delta_1(M) + \Delta_2(M) \ll Q(N)Q(M), \end{aligned} \tag{2.4}$$

where $M := N - j \ge 1$, suffices to complete the proof. By virtue of (1.7), we have

$$\Delta_2(M) \ll \frac{Q(N)Q(M)}{M} \sum_{M/2<i\le M} \Big(1 - \frac{i}{M+1}\Big)^{-1/2} \ll Q(N)Q(M).$$

To estimate the sum $\Delta_1(M)$, we twice apply asymptotical formula (1.6). This and the inequality $(1-x)^{-1/2} - 1 \le 2x$ for $0 \le x \le 1/2$ yield

$$\begin{aligned} \Delta_1(M) &= Q(N)Q(M) \sum_{i\le M/2} \frac{1}{i} \Big[\Big(1 - \frac{i}{M}\Big)^{-1/2} \Big(1 + O\Big(\frac{1}{M}\Big)\Big) \\ &\qquad - \Big(1 - \frac{i}{N}\Big)^{-1/2} \Big(1 + O\Big(\frac{1}{N}\Big)\Big) \Big]^+ \\ &= Q(N)Q(M) \sum_{i\le M/2} \frac{1}{i} O\Big(\frac{i}{M}\Big) \ll Q(N)Q(M). \end{aligned}$$

Adding the estimates of $\Delta_1(m)$ and $\Delta_2(m)$, we obtain (2.4). Theorem 1.1 is proved.

Proof of Theorem 1.2 Observe that we may take $h_j(s) = 0$ for $js > N$, since these values never appear in the moments of an additive function $h(\varphi)$. Moreover, it suffices to deal with nonnegative functions $h(\varphi)$ only. Formula (1.5) yields

$$\nu_N\big(k_j(\varphi) = k\big) = \frac{1}{Q(N)} \sum_{\substack{\ell(\bar{s})=N \\ s_j=k}} \prod_{i\le N} \Big(\frac{m_i}{i!}\Big)^{s_i} \frac{1}{s_i!} = \frac{\lambda_j^k \mathrm{e}^{jk} Q^{(j)}(N-jk)}{k! Q(N)}.$$

Hence

$$\mathbf{E}_N h(\varphi) = \sum_{jk \le N} h_j(k) \nu_N\big(k_j(\varphi) = k\big) = \sum_{jk \le N} \frac{h_j(k)\lambda_j^k}{k!} \frac{\mathrm{e}^{jk} Q^{(j)}(N - jk)}{Q(N)}$$

as claimed in (1.11).

Further, define

$$Q^{(i,j)}(M) := \sum_{\substack{\ell(\bar{s}) = M \\ s_i = s_j = 0}} \prod_{r \le M} \Big(\frac{m_r}{r!}\Big)^{s_r} \frac{1}{s_r!}$$

provided that $1 \le i < j \le M \le N$, $Q^{(i,j)}(M) := Q^{(i)}(M)$ for $i \le M < j \le N$, and $Q^{(i,j)}(M) := Q(M)$ if $M < i < j$. If $il + jk \le N$ and $i \ne j$, then

$$\nu_N\big(k_i(\varphi) = l, k_j(\varphi) = k\big) = \frac{\lambda_i^l \lambda_j^k \mathrm{e}^{il+jk} Q^{(i,j)}(N - il - jk)}{l!k!Q(N)}$$

and

$$\begin{aligned}
\mathbf{E}_N h^2(\varphi) &= \sum_{i,j \le N} h_i(l) h_j(k) \nu_N\big(k_i(\varphi) = l, k_j(\varphi) = k\big) \\
&= \sum_{jk \le N} \frac{h_j^2(k)\lambda_j^k}{k!} \frac{\mathrm{e}^{jk} Q^{(j)}(N - jk)}{Q(N)} \\
&\quad + \sum_{\substack{jk + il \le N \\ i \ne j}} \frac{h_i(l) h_j(k) \lambda_i^l \lambda_j^k}{l!k!} \frac{\mathrm{e}^{il+jk} Q^{(i,j)}(N - il - jk)}{Q(N)}.
\end{aligned}$$

Omitting a part of the nonnegative summands we have

$$\Big(\mathbf{E}_N h(\varphi)\Big)^2 \ge \sum_{jk + il \le N} \frac{\lambda_i^l h_j(l)}{l!} \frac{\mathrm{e}^{il} Q^{(i)}(N - il)}{Q(N)} \frac{\lambda_j^k h_j(k)}{k!} \frac{\mathrm{e}^{jk} Q^{(j)}(N - jk)}{Q(N)}.$$

The last two relations imply

$$\begin{aligned}
\mathbf{V}_N h(\varphi) \le D^2(N) &+ \sum_{jk + il \le N} \frac{\lambda_i^l h_j(l)}{l!} \frac{\lambda_j^k h_j(k)}{k!} \\
&\times \mathrm{e}^{il+jk} \left(\frac{Q^{(i,j)}(N - il - jk)}{Q(N)} - \frac{Q^{(j)}(N - jk) Q^{(i)}(N - il)}{Q(N)^2} \right)^+
\end{aligned}$$

$$\le D^2(N) + \sum_{jk<N} \frac{\lambda_j^k h_j^2(k) \mathrm{e}^{jk}}{k!}$$
$$\times \sum_{il \le N-jk} \frac{\lambda_i^l}{l!} \mathrm{e}^{il} \left(\frac{Q^{(i,j)}(N-il-jk)}{Q(N)} - \frac{Q^{(j)}(N-jk) Q^{(i)}(N-il)}{Q(N)^2} \right)^+.$$

In the last step, we again applied the inequality $ab \le (a^2 + b^2)/2$. It remains to estimate the inner sum. Namely, we have to prove that

$$S(M) := \sum_{il \le M} \frac{\lambda_i^l}{l!} \left(\frac{\mathrm{e}^{il} Q^{(i,j)}(M-il)}{Q(M)} - \frac{Q^{(j)}(M)}{Q(M)} \frac{\mathrm{e}^{il} Q^{(i)}(N-il)}{Q(N)} \right)^+ \ll 1 \tag{2.5}$$

for $1 \le M := N - jk < N$ and $j \le N-1$. The sum over $M/2 < il \le M$ does not exceed

$$\frac{1}{Q(M)} \sum_{M/2 < il \le M} \frac{\lambda_i^l \mathrm{e}^{il}}{l!} Q^{(i)}(M-il)$$
$$= \frac{1}{Q(M)} \sum_{M/2 < il \le M} \frac{\lambda_i^l \mathrm{e}^{il}}{l!} \sum_{\substack{\ell(\bar{t}) = M-il \\ t_i = 0}} \prod_{r \le M-il} (\mathrm{e}^r \lambda_r)^{t_r} \frac{1}{t_r!} \le 1.$$

The estimation of the remaining sum in (2.5) over $il \le M/2$ is more subtle. We need asymptotic formulae for the quantities in the difference

$$R(i,l) := \frac{\mathrm{e}^{il} Q^{(i,j)}(M-il)}{Q(M)} - \frac{Q^{(j)}(M)}{Q(M)} \frac{\mathrm{e}^{il} Q^{(i)}(N-il)}{Q(N)}$$

with remainders estimated uniformly in $j \le N-1$. For brevity, let

$$q(n) = \mathrm{e}^{-n} Q(n), \qquad q^{(j)}(n) = \mathrm{e}^{-n} Q^{(j)}(n), \qquad q^{(i,j)}(n) = \mathrm{e}^{-n} Q^{(i,j)}(n).$$

In our notation,

$$\sum_{n=0}^{\infty} q^{(j)}(n) z^n = \mathrm{e}^{-\lambda_j z^j} \sum_{n=0}^{\infty} q(n) z^n,$$

where the two series converge in $|z| < 1$. Let

$$\mathrm{e}^{-\lambda_j z^j} =: \sum_{m=0}^{\infty} c_m(j) z^m,$$

then $c_m(j) = 0$ if $j \not| m$. Moreover, since $\lambda_j \le Cj^{-1}$ with an absolute positive constant C, we have $c_m(m) = -\lambda_m \ll m^{-1}$ if $m \ge 1$ and

$$\big|c_m(j)\big| = \lambda_j^{m/j}\frac{1}{(m/j)!} \ll \Big(\frac{Ce}{m}\Big)^{m/j} \ll \frac{1}{m^2} \tag{2.6}$$

provided that $m \ge 1$, $j|m$, $j \ne m$ and hence $j \le m/2$. Applying the routine convolution argument, we firstly split

$$q^{(j)}(n) = \Big(\sum_{0\le k\le n/2} + \sum_{n/2<k\le n}\Big)c_k(j)q(n-k) = \Sigma_1 + \Sigma_2,$$

then using (1.6) and (2.6), we deduce that

$$\begin{aligned}\Sigma_1 &= \frac{1}{\sqrt{2\pi n}}\sum_{0\le k\le n/2} c_k(j) + \frac{1}{\sqrt{2\pi}}\sum_{0\le k\le n/2} c_k(j)\Big(\frac{1}{\sqrt{n-k}} - \frac{1}{\sqrt{n}}\Big) + O\Big(\frac{1}{n^{3/2}}\Big)\\ &= \frac{\mathrm{e}^{-\lambda_j}}{\sqrt{2\pi n}} + O\Big(\frac{\log(n+1)}{n^{3/2}}\Big) = \mathrm{e}^{-\lambda_j}q(n)\Big(1 + O\Big(\frac{\log(n+1)}{n}\Big)\Big)\end{aligned}$$

uniformly in $j \le n$. For the remaining sum we observe

$$\Sigma_2 \ll \mathbf{1}\{n/2 < j \le n\}\frac{1}{j} + \frac{1}{n^2}\sum_{1\le k\le n/2}\frac{1}{\sqrt{k}} \ll \frac{1}{n}.$$

Consequently,

$$q^{(j)}(n) = \mathrm{e}^{-\lambda_j}q(n)\Big(1 + O\Big(\frac{1}{\sqrt{n}}\Big)\Big). \tag{2.7}$$

The same argument, by virtue of a relation

$$\sum_{n=0}^{\infty} q^{(i,j)}(n)z^n = \mathrm{e}^{-\lambda_i z^i}\sum_{n=0}^{\infty} q^{(j)}(n)z^n$$

and the just obtained estimate (2.7), gives

$$q^{(i,j)}(n) = \mathrm{e}^{-\lambda_j}q^{(i)}(n)\Big(1 + O\Big(\frac{1}{\sqrt{n}}\Big)\Big) = \mathrm{e}^{-\lambda_i-\lambda_j}q(n)\Big(1 + O\Big(\frac{1}{\sqrt{n}}\Big)\Big). \tag{2.8}$$

Inserting (2.7) for $n = M$ and $n = N - il$ together with (2.8) for $n = M - il \ge M/2$ into $R(i, j)$, we obtain

$$\begin{aligned} R(i,l) &= \mathrm{e}^{-\lambda_i-\lambda_j}\left(\frac{q(M-il)}{q(M)} - \frac{q(N-il)}{q(N)} + O\Big(\frac{1}{M}\Big)\right) \\ &\ll \mathrm{e}^{-\lambda_i-\lambda_j}\left(\Big(1-\frac{il}{M}\Big)^{-1/2} - \Big(1-\frac{il}{N}\Big)^{-1/2} + \frac{1}{M}\right) \\ &\ll \mathrm{e}^{-\lambda_i}\frac{il}{M}. \end{aligned}$$

provided that $il \le M/2$.

Returning to (2.5), we observe that

$$\begin{aligned} S(M) &\ll 1 + \sum_{il\le M/2} \frac{\lambda_i^l}{l!} R(i,l) \ll 1 + \frac{1}{M}\sum_{i\le M/2} i\mathrm{e}^{-\lambda_i} \sum_{l=1}^{\infty} \frac{l\lambda_i^l}{l!} \\ &\ll 1 + \frac{1}{M}\sum_{i\le M/2} i\lambda_i \ll 1. \end{aligned}$$

This completes the proof of Theorem 1.2.

Concluding Remarks The applied approach still works if a mapping $\varphi \in \mathbf{T}_N$ is sampled according to a weighted multiplicative probability $P_N(\{\varphi\})$, say,

$$P_N(\{\varphi\}) = \frac{1}{C_N}\prod_{j\le N} \theta_j^{k_j(\varphi)},$$

where $\theta_j \ge 0$ are constants satisfying some regularity conditions and C_N stands for a normalizing sequence. In recent years a few new models of random mappings were introduced (see, for example, [6] or more recent papers); however, they do not fall into the discussed class.

Going along the path, analogues of the Turán-Kubilius inequality can be obtained for classes of assemblies (see [1] for a definition) generalizing permutations and mappings. For the so-called additive arithmetical semigroups, fairly general results have been obtained by S. Wehmeier [13]. Estimations of general moments of additive functions defined on mappings, similar to that elaborated in number theory by P.D.T.A. Elliott, A. Hildebrand, I.Z. Ruzsa, K.-H. Indlekofer and I. Kátai, would be highly desirable.

References

1. R. Arratia, A.D. Barbour, S. Tavaré, *Logarithmic Combinatorial Structures: A Probabilistic Approach*. EMS Monographs in Mathematics (EMS Publishing House, Zürich, 2003)
2. A. Biró, T. Szamuely, A Turán-Kubilius inequality with multiplicative weights. Acta Math. Hung. **70**(1–2), 39–56 (1996)
3. P.D.T.A. Elliott, *Duality in Analytic Number Theory* (Cambridge University Press, Cambridge, 1997)
4. P. Flajolet, R. Sedgewick, *Analytic Combinatorics* (Cambridge University Press, Cambridge, 2009)
5. J.C. Hansen, A functional central limit theorem for random mappings. Ann. Probab. **17**(1), 317–332 (1989); Correction. Ann. Probab. **19**(3), 1393–1396 (1991)
6. J.C. Hansen, J. Jaworski, A random mapping with preferential attachment. Random Struct. Algorithms **34**(1), 87–111 (2009)
7. J. Kubilius, *Probabilistic Methods in the Theory of Numbers*. Translations of Mathematical Monographs, vol. 11 (American Mathematical Society, Providence, 1964)
8. E. Manstavičius, Stochastic processes with independent increments for random mappings. Lith. Math. J. **39**(4), 393–407 (1999)
9. E. Manstavičius, On the random mapping statistics, in *Elementare und Analytische Zahlentheorie (Tagungsband) Proceedings ELAZ-Conference*, May 24–28, 2004, ed. by W. Schwarz, J. Steuding (Hg.) (Franz Steiner Verlag, Stuttgart, 2006), pp. 180–191
10. E. Manstavičius, Moments of additive functions on random permutations. Acta Appl. Math. **97**, 119–127 (2007)
11. E. Manstavičius, On total variation approximations for random assemblies, in *23rd International Meeting on Probabilistic, Combinatorial, and Asymptotic Methods for the Analysis of Algorithms (AofA'12)*, ed. by N. Broutin, L. Devroye (Association of Discrete Mathematics & Theoretical Computer Science, Nancy, 2012), pp. 97–108
12. E. Manstavičius, V. Stepanauskas, On variance of an additive function with respect to a generalized Ewens probability, in *Proceeding of 25th International Conference on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AofA'14)*, ed. by M. Bousquet-Mélou, M. Soria. DMTCS-HAL Proceedings Series (2014), pp. 301–312
13. S. Wehmeier, Die Turán-Kubilius Ungleichung für additive arithmetische Halbgruppen. Liet. Matematikos Rinkinys **46**(3), 457–471 (2006); Translation in: Lith. Math. J. **46**(3), 371–383 (2006)

Aspects of Zeta-Function Theory in the Mathematical Works of Adolf Hurwitz

Nicola Oswald and Jörn Steuding

Dedicated to the Memory of Prof. Dr. Wolfgang Schwarz

Abstract Adolf Hurwitz is rather famous for his celebrated contributions to Riemann surfaces, modular forms, diophantine equations and approximation as well as to certain aspects of algebra. His early work on an important generalization of Dirichlet's *L*-series, nowadays called Hurwitz zeta-function, is the only published work settled in the very active field of research around the Riemann zeta-function and its relatives. His mathematical diaries, however, provide another picture, namely a lifelong interest in the development of zeta-function theory. In this note we shall investigate his early work, its origin, and its reception, as well as Hurwitz's further studies of the Riemann zeta-function and allied Dirichlet series from his diaries. It turns out that Hurwitz already in 1889 knew about the essential analytic properties of the Epstein zeta-function (including its functional equation) 13 years before Paul Epstein.

Keywords Adolf Hurwitz • Entire functions • Riemann hypothesis • Zeta- and *L*-functions

2010 Mathematics subject classification: Primary 01A70; Secondary 01A55, 11M06, 11M35

N. Oswald
Department of Mathematics and Informatics, University of Wuppertal, Gaußstr. 20, 42 119 Wuppertal, Germany
e-mail: oswald@uni-wuppertal.de

J. Steuding (✉)
Institut für Mathematik, Universität Würzburg, Würzburg, Germany
e-mail: steuding@mathematik.uni-wuerzburg.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_20

1 Hildesheim: The Hurwitz Zeta-Function

Adolf Hurwitz was born in Hildesheim on 26 March 1859 into a Jewish family of merchants. At the age of 17 he had his first publication in mathematics, a joint paper on enumerative geometry with his Hildesheim school teacher Hermann Caesar Hannibal Schubert, a well-known geometer of the time. On promotion of Schubert young Hurwitz started his studies at the polytech university of Munich[1] in 1877 under the supervision of the eminent Felix Klein; soon after he moved with Klein to Leipzig where he obtained his doctorate in 1881.

> Being a young doctor, in the winterterm 81/82 he moved to the University of Berlin to improve himself by Weierstrass and Kronecker with whom he also had personal contact. Weierstrass was in particular interested in his doctoral thesis and his function-theoretical efforts, he also proposed the topic for his habilitation thesis.[2]

wrote Ida Samuel-Hurwitz, the later wife of Adolf Hurwitz in her dossier [96]. At Leipzig first obstacles appeared. According to Rowe: "to pursue an academic career meant applying to habilitate, and the Leipzig regulations required applicants to be graduates of a humanistic gymnasium. Klein must have realized that this stipulation, together with Hurwitz's Jewish confession, virtually ruled out any chance of his habilitating in Leipzig.", [94, p. 23].[3] Consequently, Hurwitz moved to Göttingen for his habilitation in 1882.

His first thoughts about the Riemann zeta-function and related questions fall into this period. At this time of his career Adolf Hurwitz often visited his nearby

[1] Called the *Königlich Bayerische Technische Hochschule München* which had been renamed to Technische Universität München in 1970.

[2] "Für das Wintersemester 1981/1982 bezog er als junger Doktor nochmals die Universität Berlin, um sich bei Weierstraß und Kronecker, zu denen er auch in persönliche Beziehung trat, noch weiter zu vervollkommnen. Weierstraß interessierte sich besonders für seine Dissertation und seine funktionentheoretischen Bestrebungen, auch gab er ihm das Thema für die Habilitation daselbst...", [96, p. 6]; this translation from the original German quotation to English as well as those in the sequel are due to the authors; we have neither corrected the German language to the grammar used nowadays nor have we tried to translate into old-fashioned English. The mentioned university is the *Humboldt University*, before 1949 called *Friedrich-Wilhelms-Universität*.

[3] Even stronger is a statement of Ida Samuel-Hurwitz about anti-Semitism at Leipzig University during Hurwitz's lifetime: "Obgleich sein mangelhafter Gesundheitszustand natürlich bekannt war, trachtete man in Deutschland mehrfach, ihn wieder dorthin zu ziehen. Als gleichwertig mit seinem Zürcher Lehrstuhl, den nacheinander eine Reihe der hervorragendsten Mathematiker bekleidet hatten, konnten freilich nur Berlin, München und Leipzig in Frage kommen. An die letzte Universität war die Berufung eines Juden ausgeschlossen; für Berlin war er bei Vakanz an erster Stelle vorgeschlagen. Von Göttingen war natürlich öfters die Rede, doch scheute er einerseits den mathematischen Betrieb dort, während ihm andererseits die Kleinstadt unsympatisch war." [96, p. 11]. English translation: "Although his defective health was known there were attempts to get him back to Germany. As equivalent to his Zurich chair only Berlin, Munich and Leipzig could be considered. To fill a vacant professorship with a Jew at the latter university was impossible; for Berlin he was recommend for the first place in case of a vacancy. Of course, Göttingen was often under discussion, but on one side he disliked the mathematical business there, on the other side he considered the small town unsympathetic."

Fig. 1 Adolf Hurwitz (1859–1919) in between his teachers Felix Klein (1849–1925) on the *left* and Karl Weierstrass (1815–1897) on the *right*. The photographs seem to be taken around 1881. Besides Klein, Hurwitz had been significantly influenced by the Berlin school

hometown Hildesheim. From several letters to his friend from his studies at Munich University (and later renown analyst) Luigi Bianchi one can get interesting insights about this period. In a letter from 25 May 1882, Adolf Hurwitz had already finished his habilitation and had been working as a private docent in Göttingen, he wrote to Bianchi:

> Instantly I am visiting home for Pentecost which I can allow myself since Hildesheim can be reached by train from Göttingen within 2 hours (...) In Göttingen, I live a pleasant life. Prof. H.A. Schwarz is very kind to me and Dr. v. Mangoldt, who is a privat docent for mathematics as well, is a very noble character. Furthermore, in math at Göttingen there is Prof. Stern and Prof. Schering.[4]

In particular Hans von Mangoldt (1854–1925) is interesting here. He played an important role in zeta-function theory and its application to questions about prime numbers; his contributions in the 1890s turned out to be essential for the first proof of the prime number theorem in 1896 (details in Sect. 2). Here, the Riemann zeta-function

$$\zeta(s) := \sum_{n\geq 1} n^{-s} = 1 + 2^{-s} + 3^{-s} + 4^{-s} + \dots$$

is building the bridge between primes on the arithmetical side and the powerful tools of complex analysis on the other side. It was young Adolf Hurwitz who

[4] "Augenblicklich bin ich auf Pfingsten zu Besuch zu Hause, was ich mir um so eher erlauben kann, als Hildesheim von Göttingen aus in 2 Stunden per Eisenbahn zu erreichen ist. (...) In Göttingen führe ich ein sehr angenehmes Leben. Prof. H.A. Schwarz ist sehr nett gegen mich und Dr. v. Mangoldt, welcher ebenfalls Privatdoc. für Mathematik ist, ist ein sehr nobler Character. Ferner sind von Mathemat. in Göttingen noch Prof. Stern und Prof. Schering."

invented already in 1881 a simple but important generalization, the nowadays so-called Hurwitz zeta-function, given by

$$\zeta(s,\alpha) := \sum_{m\geq 0}(m+\alpha)^{-s}, \tag{1.1}$$

where α is a real parameter satisfying $0 < \alpha \leq 1$. Actually Hurwitz just considered the case of rational α which is sufficient for applications to number theory; however, for most studies general real numbers α do not cause big trouble. We notice that the series representation from above is absolutely convergent for $\operatorname{Re} s > 1$, uniformly in any compact subset.

We believe that the years 1881–1884 played a very important role in Adolf Hurwitz's life. Of course, he did his doctorate and his habilitation in this period, and in addition he started his important investigations on several topics different to the themes of his doctoral and habilitation theses (on modular forms). With his studies of the Hurwitz zeta-function as well as of real and complex continued fractions he emancipated from his advisor Klein (as well as from his mentor Weierstrass in Berlin) and became an independent mathematician. Concerning continued fractions this is well documented in Oswald and Steuding [78]. In this chapter we focus on Hurwitz's work on the Riemann zeta-function and its relatives.

1.1 Prehistory: From Euler to Riemann

The infinite series $1 + 2^{-s} + 3^{-s} + \ldots$ defining the zeta-function is linked with the name Leonhard Euler in many ways. Starting from 1735, he gave various proofs of his famous formula $\zeta(2) = \frac{\pi^2}{6}$; in 1743 he found explicit values for $\zeta(s)$ at the positive even integers [24], namely

$$\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k} \qquad \text{and} \qquad \zeta(1-2k) = -\frac{B_{2k}}{2k},$$

both valid for integral k, although Euler had no convergent representation for $\zeta(s)$ when s is a negative real. The numbers B_m are the Bernoulli numbers. Concerning the functional equation linking the values $\zeta(s)$ and $\zeta(1-s)$, Euler claimed that there is no doubt about the truth of this conjecture [25].[5] Most importantly, although elementary, in 1737 Euler [23] discovered the analytical analogue of the unique prime factorization in terms of $\zeta(s)$ by observing

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_{p\in\mathbb{P}}(1-p^{-s})^{-1},$$

[5] Euler's approach has led to a powerful tool in theoretical physics, called regularization; it was Stephen Hawking [42] in 1977 who was the first to use the Riemann zeta-function by this method in order to compute certain quantities in quantum field theory.

valid for $\operatorname{Re} s > 1$ (the half-plane of absolute convergence for both, the series and the product), where $\mathbb{P}$ denotes the set of prime numbers. The appearing product is named after Euler and had been used by himself to deduce from the divergent harmonic series (appearing as $\zeta(s)$ with $s \to 1+$) the existence of infinitely many primes by his famous formula

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots = \log\log\infty$$

(which nowadays is written as $\sum_{p \le x; p \in \mathbb{P}} \frac{1}{p} \sim \log\log x$).[6]

The function $\zeta(s)$, however, is named after Bernhard Riemann who was the first to study the behavior of $\zeta(s)$ as a function of a complex variable in his path-breaking nine pages article [93] written at the occasion of his admission to the Prussian Academy of Sciences in 1859. He proved analytic continuation for $\zeta(s)$ to the whole complex plane except for a simple pole at $s = 1$ and Euler's conjectured functional equation[7]

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s);$$

Indeed, Riemann gave two rather different proofs of the functional equation, the first one by use of a certain contour integral (which will be the main topic of this section when we shall analyze Hurwitz's paper) and another one based on Poisson's summation formula and Jacobi's transformation formula for the theta-function.[8] It follows from the functional equation and basic properties of the gamma-function that the nontrivial zeros (i.e., the non-real zeros) are symmetrically distributed with respect to the real axis and the so-called critical line $\operatorname{Re} s = \frac{1}{2}$. However, Riemann's paper [93] is probably more important with respect to its not rigorously proved statements and conjectures. Nowadays this very memoir has been considered as a signpost for developing complex analytic methods in order to reveal distribution properties of the prime numbers.

> Analytic number theory may be said to begin with the work of Dirichlet, and in particular with Dirichlet's memoir of 1837 on the existence of primes in a given arithmetic progression.

This quotation is the first sentence in Davenport's monography on *multiplicative number theory* [13], referring to the celebrated work of Johannes Peter Gustav

[6] It should be noted that Euler used slightly different notation. For more details on Euler's work we refer to Weil [112].

[7] According to Landau [58], the only other mathematician to have noticed Euler's work on this topic had been Cahen [9]. This statement is refuted by Malmstèn [70], nevertheless some of Euler's works were probably not easily accessible in this time. Only the era of mathematical journals made an easy exchange of mathematical ideas possible.

[8] It was shown by Hamburger [38] that a functional equation of the Riemann-type is equivalent to both, the Poisson summation formula and a theta-function transformation formula.

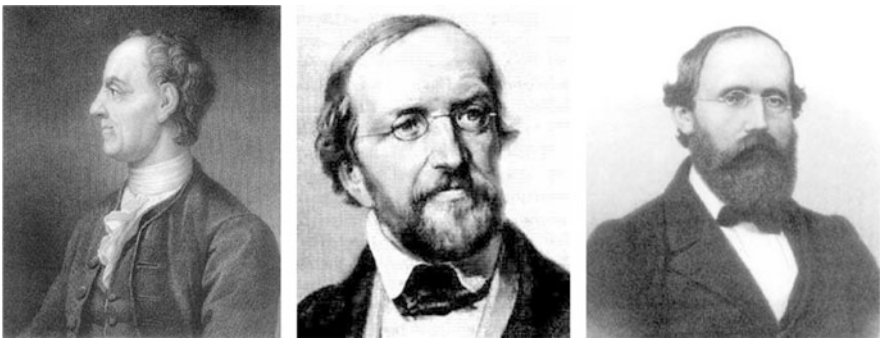


Fig. 2 From *left* to *right* the pioneers of analytic number theory: Leonhard Euler (1707–1783), Peter Gustav Lejeune Dirichlet (1805–1859), and Bernhard Riemann (1826–1866). Beards seem to have been pretty much in fashion in the nineteenth century

Lejeune Dirichlet on the distribution of primes in arithmetic progressions, resp. prime residue classes around 1837, about one generation before Riemann. In fact, if one seeks for primes in the residue classes modulo 4, one observes a certain uniform distribution of the primes in the prime residue classes:

$$
\begin{aligned}
4\mathbb{Z}+1 &: \ldots 1\ \mathbf{5}\ 9\ \mathbf{13}\ \mathbf{17}\ldots\\
4\mathbb{Z}+2 &: \ldots \mathbf{2}\ 6\ 10\ 14\ 18\ldots \leftarrow \text{just one prime}\\
4\mathbb{Z}+3 &: \ldots \mathbf{3}\ \mathbf{7}\ \mathbf{11}\ 15\ \mathbf{19}\ldots\\
4\mathbb{Z}+0 &: \ldots 4\ 8\ 12\ 16\ 20\ldots \leftarrow \text{no prime at all}
\end{aligned}
$$

Notice that Euclid's celebrated proof of the infinitude of primes cannot be extended to prove the existence of infinitely many primes in an arbitrary prime residue class $a \bmod m$; actually, as proved by Ram Murty (see [76] for a recent presentation) such an elementary proof is possible if and only if $a^2 \equiv 1 \bmod m$. A first attempt for proving an infinitude of primes in a prime residue class was given by the unfortunate Adrien Marie Legendre [64]; however, his proof was erroneous, and this was pointed out by Dirichlet [18] himself. Before we outline Dirichlet's work on primes in arithmetic progressions we shall briefly mention the circumstances under which Dirichlet wrote his landmark paper [18] on this topic (building on Elstrodt's biography [21]).

His given name *Lejeune* means literally *the young* and his surname *Dirichlet* provides information about the origin of his family being *from Richelette*, a small town in Belgium.[9] His school and university education benefited a lot from the

[9]There is something funny about his birthplace: Dirichlet was born in Düren, in between Aachen and Cologne, and the house his mother gave birth is *Weierstraße 17*; notice that *Straße* is German for *street* and the mathematician and contemporary Karl Weierstrass is written *Weierstraß* in German.

reform of the Prussian educational system implemented by Wilhelm von Humboldt. In 1828, his brother Alexander von Humboldt used his influence to order the young Dirichlet to Berlin.[10] Starting from 1831 Dirichlet had a research position at the University of Berlin[11] and in the following year he was elected member of the Prussian Academy of Science. In the same year he married Rebecka Mendelssohn, a sister of the composers Fanny Hensel (the grandmother of the number theorist Kurt Hensel) and Felix Mendelssohn Bartholdy.[12] For the last 4 years of his short life Dirichlet inherited Carl Friedrich Gauss' chair at the University of Göttingen.

One of his major results is the proof of the existence of infinitely many prime numbers in arbitrary arithmetic progressions $a + m\mathbb{Z}$ with (of course) coprime a and m. The main idea is the use of the so-called Dirichlet characters, i.e., group homomorphisms $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ in order to sift a prime residue class a mod m. Extending these characters to arithmetical functions $n \mapsto \chi(n)$ defined on $\mathbb{N}$ (by letting $\chi(n) = 0$ for n not coprime with m), he defined associated Dirichlet series by

$$L(s, \chi) := \prod_{p \in \mathbb{P}} (1 - \chi(p)p^{-s})^{-1} = \sum_{n \geq 1} \chi(n) n^{-s};$$

the representations converge for $\operatorname{Re} s > 1$ absolutely and the identity between the product and the series is (as in the case of the Riemann zeta-function which appears essentially as $L(s, \chi_0)$ with the principal character χ_0 being constant one) nothing but the unique prime factorization in analytic disguise. Using this in combination with the orthogonality relation for characters, one finds

$$\sum_{p \equiv a \bmod m} p^{-s} \sim \frac{1}{\varphi(m)} \Big(\log \zeta(s) + \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \overline{\chi}(a) \log L(s, \chi) \Big).$$

Now the divergence of $\zeta(s)$ for $s \to 1+$ and the regularity and non-vanishing of the values $L(s, \chi)$ with $\chi \neq \chi_0$ at $s = 1$ yield the desired statement.

Dirichlet's approach is rather explicit. In the case of prime moduli $m = p$ his characters are defined by primitive roots and therefore his reasoning for showing $L(1, \chi) \neq 0$ is first limited to such restricted arithmetic progressions. The first appearance of characters can be found in Gauss' work on cyclotomy [30], the modern theory of characters starts with Richard Dedekind and his supplements to Dirichlet's lectures on number theory [20], and the general theory of characters (also for finite nonabelian groups) and group representations is due to Georg Frobenius [28]. For the general and more advanced case of composite moduli Dirichlet built his reasoning on binary quadratic forms $aX^2 + bXY + cY^2$. For the number $h(D)$ of

[10] See [6] for their intensive exchange of letters.

[11] Once again the Humboldt University, formerly Friedrich Wilhems University.

[12] The additional surname *Bartholdy* had been added to the Jewish surname with respect to the Christian education of the children, a rather common assimilation in these anti-Semitic times.

Fig. 3 From *left* to *right*: Carl Johan Malmstèn (1814–1886), Ferdinand Gotthold Max Eisenstein (1823–1852), and Oscar Xaver Schlömilch (1823–1901)

equivalence classes of these forms with fixed discriminant $D = b^2 - 4ac$ he proved the celebrated analytic class number formula [19],[13] for example

$$h(D) = \frac{\omega}{2\pi}\sqrt{-D}L(1, \chi_D)$$

for the case $D < 0$ of positive definite forms, where ω denotes the number of units in the ring of integers of $\mathbb{Q}(\sqrt{D})$ and χ_D is a quadratic character defined by the Kronecker symbol $\chi_D(n) = (\frac{D}{n})$. Since $h(D) \geq 1$ this proves $L(1, \chi_D) \neq 0$, and another subtle reasoning shows that also the non-quadratic characters do not cause any trouble. Dirichlet's reasoning is precise but more complicated than necessary since he used the Jacobi symbol in place of Kronecker's symbol. Anyway, "Dirichlet's papers, as outstanding for mathematical rigor as Euler had been careless about such matters, ..." wrote Weil [112, p. 7]. The first completely analytic proof of the non-vanishing of $L(1, \chi)$ is due to Franz Mertens [73] and uses the Dedekind zeta-function associated with quadratic number fields.

Often Schlömilch is given credit for the first significant contribution to the analytic theory of L-functions beyond Dirichlet's paper. Oscar Xaver Schlömilch was a pupil of Dirichlet; in 1845 he was appointed a professorship at the University of Jena. In 1856, he founded the *Zeitschrift für Mathematik und Physik*, also known as *Schlömilchs Zeitschrift*, and used this journal to publish several of his results.[14]

[13]It has been observed by Minkowski [74, p. 456] that already in Gauß' estate one can find a note from 1801 about the class number formula about 40 years previous to Dirichlet, however, a proof is missing; moreover, the Disquisitions [30, p. 369 and 466] contain formulae for sums of class numbers without a proof which was first delivered by Siegel [107].

[14]This periodical was only the third one published in Germany after the renowned Crelle journal established in 1826 and run by the Berlin mathematical school, and the less known *Archiv für Mathematik und Physik* founded in 1841 by Johann August Grunert in Greifswald. According to Koch [56], the reputation of Schlömilch's journal was not very good.

In 1849, Schlömilch announced in [100] the proof of the functional equation

$$L(1-s) = \left(\frac{2}{\pi}\right)^s \Gamma(s)\sin(\tfrac{\pi s}{2})L(s),$$

where $L(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} \pm \ldots$ is the Dirichlet L-function to the non-principal character χ mod 4; the proof, however, was published only in 1858 in his journal as [101] although the title of his announcement [100] is literally "Exercises for pupils concerning a theorem due to Prof. Dr. Schlömilch." In 1878, he was the first to give a proof of the functional equation for $\zeta(s)$ differing essentially from Riemann's methods [102]. Notice that Schlömilch was active in educational politics serving from 1874 until 1885 as consultant for the Saxonian Ministery of Education. For more details to his life we refer to Cantor's obituary [10].

However, it was Carl Johan Malmstèn being the first to publish a proof of a functional equation for a Dirichlet L-function. Interestingly, Malmstèn's biography shares quite many similarities with Schlömilch's. Since 1842 Malmstèn was professor at the University of Uppsala, and he was among the founders of the renowned journal *Acta Mathematica*. He was active as rector of his university as well as privy council and member of the Swedish Reichstag (parliament) for the period 1867–1870. He is famous for his contributions to the Swedish old-age pension insurance and he was member of the Royal Prussian Academy of Sciences as well as the Göttingen Academy of Sciences; actually, his daughter Maria Heliodora was married since 1876 to the Göttingen mathematician Ernst Christian Julius Schering. In 1849, Malmstèn [70] published a proof of the functional equation for $L(s)$ independent of Schlömilch; moreover he announced that a similar reasoning would prove a corresponding result for

$$(1 - 2^{1-s})\zeta(s) = 1 - 2^{-s} + 3^{-s} - 4^{-s} \pm \ldots.$$

Actually, Malmstèn's paper bears the date "Upsala 1st May 1846." It might also be interesting to note that he used already the variable s as Riemann later, which might indicate that Riemann was aware of Malmstèn's contribution.

But the story before Riemann's memoir appeared is not yet complete. It was Ferdinand Gotthold Max Eisenstein who gave another proof of a functional equation for a Dirichlet L-function and this might have been inspiration for Riemann, too. Eisenstein was another pupil of Dirichlet and member of the Berlin and Göttingen Academies of Sciences, the latter one on promotion by Gauss. It was Andre Weil who found in 1989 in Eisenstein's copy of Gauss' *Disquisitiones Arithmeticae* on the last and blank page a hand-written proof of the functional equation for $L(s)$ bearing the date "Scripsi 7 April 1849" (cf. [112, 113]), the time when Riemann left Berlin for Göttingen. Eisenstein's proof is based on Poisson's summation formula as the second one given by Riemann. It is well known that Riemann was attending Eisenstein's lectures on elliptic functions in Berlin in the summer 1847 but it seems

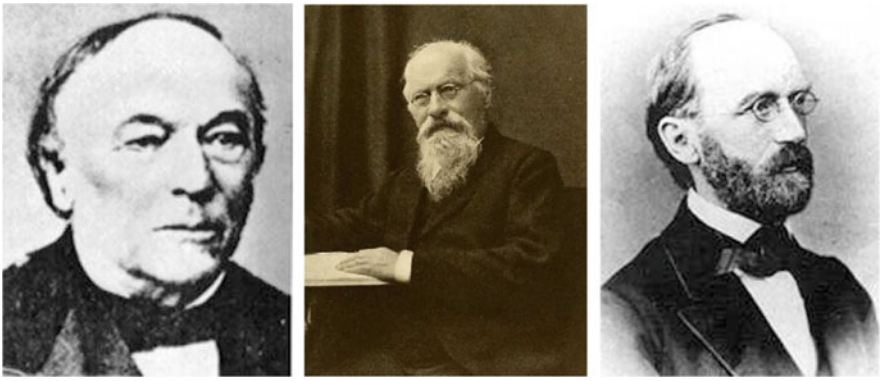


Fig. 4 Thomas Clausen (1801–1885), Hermann Kinkelin (1832–1912), and Wilhelm Scheibner (1826–1908). Nowadays only the astronomer and mathematician Clausen is still well known. Beards again: two out of three

that their relation was not too good.[15] Why did Riemann give two different proofs for the functional equation? Of course, we may only speculate, but a possible answer could be to convince himself about the truth of the result; a further reply could be to stress the importance, and yet another possibility could be awareness of such a result (e.g., Eisenstein's proof).

In 1858 Thomas Clausen [11], and in 1862 Hermann Kinkelin [55] gave alternative proofs for the functional equation for $L(s)$ and generalizations thereof, respectively. Clausen's work [11] is related to his studies of Bernoulli numbers. Kinkelin was a Swiss mathematician working essentially in analysis until 1865; later he focused on didactics and mathematics for insurances. In 1865, he was appointed a professorship at the University of Basel.[16] Also Kinkelin was politically active (for a conservative party), and in 1886 he was elected Senior Civil Servant (see Schaertlin [97] for details). His studies [55] from 1862 include a proof of the functional equation for $L(s, \chi)$ for characters χ mod q with q being a prime power or a squarefree odd integer. Kinkelin is not often cited; we can find a note of his work in Landau's *Handbuch* [59].[17] Though no comment about the arithmetical implications of Riemann's paper is given. It might be that some people of that time

[15]The quotation "Eisenstein stopped at formal computation" (resp. in German: "Eisenstein sei bei der formellen Rechnung stehengeblieben") is credited to Riemann; cf. Laugwitz [63, p. 21].

[16]Where around 1896 also Julius Hurwitz, the less famous brother of Adolf Hurwitz, was lecturing for a couple of years; see Oswald and Steuding [78] for details of Julius' interesting life and career.

[17]It is interesting to read Kinkelin's comment on what is nowadays called the Riemann hypothesis: "The last two equations seem to be satisfied simultaneously only if its root s is of the form $1/2 + \tau\sqrt{-1}$; indeed a rigorous proof of this remark has not been given so far (cf. Riemann)"; the German original is: "Die beiden letzten Gleichungen scheinen nur dann gleichzeitig nebeneinander bestehen zu können, wenn ihre Wurzel s von der Form $1/2 + \tau\sqrt{-1}$ ist; indessen ist der strenge Beweis dieser Bemerkung noch nicht gelungen (cf. H. Riemann a.a.O.)." [55, p. 18].

considered Riemann's results already as the solution of Gauss' conjecture about the number of primes below a given magnitude. Kinkelin used the notation $K(s)$ for $\zeta(-s)$ and was very much interested in the relation between Bernoulli numbers and the special values of the zeta-function at the integers. There are further contributions to be mentioned here. Wilhelm Scheibner [99] was one of the first to analyze Riemann's work; besides he succeeded to establish the case $q = 12$. In 1857 Rudolf Lipschitz [68] gave yet another proof of the functional equation for $L(s)$, however, we shall consider his results later in another context.

Riemann [93] mentioned previous works by Euler and Pafnuty Chebychev (with respect to his elementary approach), but he did not mention Legendre, Eisenstein, Malmstèn, Schlömilch, or anybody else. We cannot be sure whether he knew about their results or not. Definitely, Riemann's insight was much deeper and his methods were far beyond what his contemporaries had at hand.

1.2 The Hurwitz Identity

Adolf Hurwitz's article [46] from 1881 starts as follows:

> (...) I achieved general formulae of the same simplicity as those found by Schlömilch and Riemann, which appear as particular cases. These general formulae might be of special interest with respect to their relation to functions playing a substantial role in Dirichlet's deep investigations concerning the number of classes of binary quadratic forms and prime numbers in an arithmetic progression.[18]

Notice that [46] was published in *Schlömilchs Zeitschrift*. Therefore, it is natural to mention Schlömilch's contribution besides Riemann and Dirichlet, however, in the whole paper neither references to Malmstén, Eisenstein, nor Kinkelin can be found.

The 22 years old young doctor Adolf Hurwitz signs his paper with the date "Hildesheim, den 10. Oktober 1881" although his scientific address at that time was Berlin. The letter exchange from this period with his friend Luigi Bianchi is very interesting for several reasons. They give the picture of two extraordinarily gifted mathematicians who kept their friendship despite the geographical distance between each other.

> Infinitely I have enjoyed to have been welcomed by your letter; your last letter with your photography (the people are stupid, they go and let them photographed) I have received too.[19]

[18] "(...) gelangte ich zu allgemeinen Formeln, die von gleicher Einfachheit sind, wie die von Schlömilch und Riemann gegebenen, und dieselben überdies als spezielle Fälle enthalten. Diese allgemeinen Formeln dürften um so mehr ein Interesse beanspruchen, als sie sich auf eben die Functionen beziehen, die bei den tiefen Untersuchungen Dirichlet's über die Anzahl der Klassen binärer quadratischer Formen und über die in einer arithmetischen Reihe enthaltenen Primzahlen eine wichtige Rolle spielen.", [46, p. 73/74].

[19] "Unendlich habe ich mich gefreut mit einem Briefe von Dir empfangen zu werden; auch Deinen letzten Brief mit Deiner Photographie (Die Leute sind dumm, sie gehen und lassen sich photografiren) habe ich erhalten", [4, p. 77].

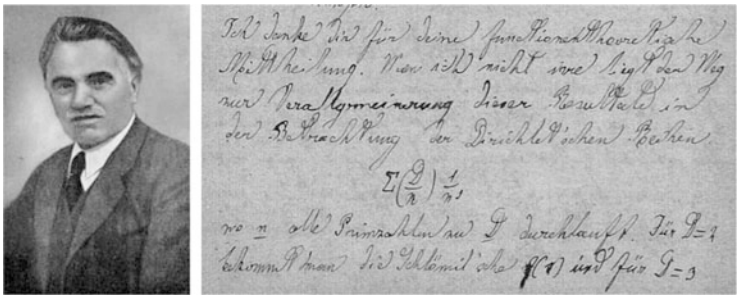


Fig. 5 On the *left* Luigi Bianchi (1856–1928) who made important contributions to differential geometry (this is probably not the photograph he sent to Hurwitz). On the *right* a part of his letter to Hurwitz with date 28 August 1881 [3]

wrote Hurwitz to Bianchi in a letter with date 23 December 1881, [4, p. 77]; a later letter of Hurwitz to Bianchi from 6 April 1883 must have contained a photograph of Hurwitz, too; [4, p. 91]. They continued writing letters to each other their whole lives, however, it seems they never met again in person. Of particular interest are mathematical topics in their correspondence. In a letter to Hurwitz with date 28 August 1881 Bianchi wrote (see Fig. 5):

> I am grateful for your function-theoretical note. If I am not wrong the path to generalize these results is in considering Dirichlet series
>
> $$\sum \left(\frac{D}{n}\right) \frac{1}{n^s}$$
>
> where n runs through all prime numbers with respect to D. For $D = 2$ one gets Schlömil(ch)'s series and for $D = 3$ one gets yours.[20]

Unfortunately, the previous letter of Adolf Hurwitz got lost; however, in [4], Opere, Vol. XI: Corrispondenza, one can read Hurwitz's reply to Bianchi from 24 September 1881:

> Your serendipity has found the correct generalization; however, I have had the same idea a few days after sending you my previous letter on my own, since the easy treatable case of a prime number had necessarily guided me. Today I shall inform you about the complete results...[21]

[20] In the subsequent paper [79] the authors investigated the Hurwitz estate further and found interesting details concerning Hurwitz's approach to zeta-functions associated with quadratic forms.

[21] "Dein Spürsinn hat die richtige Verallgemeinerung getroffen; ich hatte allerdings auch ein paar Tage nach der Absendung meines vorigen Briefes dieselbe Idee, da mich der leicht zu behandelnde Fall einer Primzahl mit Nothwendigkeit darauf führte. Ich theile Dir nun heutige die fertigen Resultate mit...", [4, p. 74].

Luigi Bianchi was a student of Enrico Betti and Ulisse Dini; he received his doctorate already in 1877. Afterwards he continued his studies at the University of Munich where he became a friend of Adolf Hurwitz. Their correspondence gives indeed a lively picture of a deep and lifelong friendship and it seems there was no competition between the two young stars.

We shall briefly outline Hurwitz's proof (using more or less his notation). First of all, given integers $1 \leq a \leq m$, he defines

$$f(s,a) := a^{-s} + (a+m)^{-s} + (a+2m)^{-s} + \ldots = \sum_{n \equiv a \bmod m} n^{-s};$$

in the now common notation (1.1) this Dirichlet series equals $m^{-s}\zeta(s, a/m)$, and we recover the Riemann zeta-function as $\zeta(s) = f(s,1)$ in the case $m = 1$. Building on Riemann's first proof of the functional equation, Hurwitz starts with Euler's integral representation of the gamma-function,

$$\Gamma(s) = \int_0^\infty t^{s-1} \exp(-t) \mathrm{d}t,$$

valid for $\mathrm{Re}\, s > 0$. Substituting $t = nx$ and summing up over $n \equiv a \bmod m$, he gets

$$\Gamma(s) \sum_{n \equiv a \bmod m} n^{-s} = \sum_{n \equiv a \bmod m} \int_0^\infty x^{s-1} \exp(-nx) \mathrm{d}x.$$

By uniform convergence, interchanging summation and integration is allowed; the resulting sum of exponentials is a geometric series with value

$$\sum_{n \equiv a \bmod m} \exp(-nx) = \sum_{k \geq 0} \exp(-(km+a)x) = \frac{\exp(-ax)}{1 - \exp(-mx)}. \tag{1.2}$$

It might be interesting to notice that already in Dirichlet's approach [18] one can find a comparable integral representation for the product of a Dirichlet series with the gamma-function. Actually, Hjalmar Mellin [71, 72] developed a theory for such integral representations coining the notion of a Mellin transform. It might be interesting to notice that in 1881/82 Mellin studied at the University of Berlin (cf. Lindelöf [67]) so he might have met Hurwitz in person when he was starting his investigations of the Hurwitz zeta-function. Previous to Mellin it was Eugène Cahen [9] who studied for his doctorate such transformations, however, his dissertation had been criticized for its many errors by Adolf Hurwitz in his review [48] for the Jahresberichte; it was later corrected by Oskar Perron [80] (who also removed some mistake of Kronecker [57]).

Betrachten wir jetzt in der Ebene der komplexen Variabeln x ein Rechteck, dessen Seiten der Axe der rein imaginären Zahlen, resp. der Axe der reellen Zahlen parallel laufen und dessen Mittelpunkt der Punkt $x = 0$ ist (Fig. 2), so wird im Innern desselben die Funktion

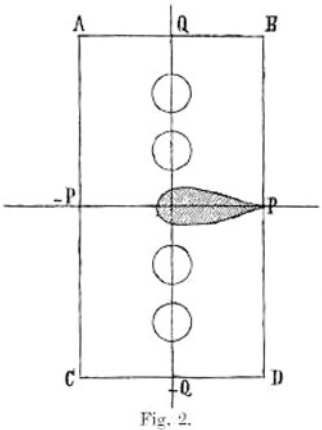


Fig. 2.

$$\psi(x) = (-x)^{s-1} \cdot \frac{e^{(m-a)x}}{e^{mx} - 1}$$

nur für die Punkte $x = \frac{2k\pi i}{m}$, $k = \pm 1, \pm 2, \ldots$ und $x = 0$ unstetig.

Fig. 6 A picture from Hurwitz's article [46] showing a drawing of the contour used in the proof of the Hurwitz identity

We continue with Hurwitz's proof. It follows from (1.2) that

$$\Gamma(s)f(s,a) = \int_0^\infty \frac{\exp((m-a)x)}{\exp(mx)-1} x^{s-1} \mathrm{d}x.$$

Now define the integral[22]

$$J(s) = \int_C \exp((s-1)\log(-x)) \frac{\exp((m-a)x)}{\exp(mx)-1} \mathrm{d}x,$$

where the contour C is the path starting from $+\infty$ along the real axis in the upper half-plane to a real point $A > 0$, then counterclockwise continuing on the circle $\circ$ of radius A around the origin and then back to $+\infty$ along the real axis in the lower half-plane; we may assume that A is so small that the only singularity of the integrand inside C is at the origin, and that there is no singularity on C. For positive

[22]Such integrals are now called Hankel integrals in honor of Riemann's pupil Hermann Hankel who used them in his studies [39] of the Gamma-function (although already Riemann [93] used them earlier).

x the imaginary part of the logarithm $\log(-x)$ is equal to $-i\pi$ on the positive part of the real axis and equal to $+i\pi$ on the negative part. Consequently,

$$J(s) = \int_A^\infty (\exp(-i\pi s) - \exp(i\pi s))x^{s-1}\frac{\exp((m-a)x)}{\exp(mx)-1}\mathrm{d}x + \\ + \int_\circ \exp((s-1)\log(-x))\frac{\exp((m-a)x)}{\exp(mx)-1}\mathrm{d}x.$$

The integral over the small circle $\circ$ tends for $\mathrm{Re}\, s > 1$ to zero as $A \to 0$, giving

$$\lim_{A\to 0} J(s) = -2i\sin(\pi s)\Gamma(s)f(s,a).$$

Using the formula

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s},$$

Hurwitz deduces

$$f(s,a) = \frac{i}{2\pi}\Gamma(1-s)\lim_{A\to 0} J(s).$$

Since the integral $\lim_{A\to 0} J(s)$ converges uniformly on compact sets it defines an entire function. Consequently, the only possible singularities of $f(s,a)$ are the poles of $\Gamma(1-s)$ at the positive integers; however, since $f(s,a)$ is obviously regular for $s = 2, 3, \ldots$, it only remains to consider the local behavior at $s = 1$. In view of $\Gamma(z+1) = z\Gamma(z)$ (which was already known to Euler) one has

$$\Gamma(1-s) = \frac{-1}{s-1} + \ldots$$

and in combination with

$$\lim_{A\to 0} J(1) = \int_0^\infty (-x)^{s-1}\frac{\exp((m-a)x)}{\exp(mx)-1}\mathrm{d}x = \frac{2\pi i}{m}$$

it follows that $f(s,a)$ *admits an analytic continuation to* $\mathbb{C}$ *except a simple pole at* $s = 1$ *with residue* $1/m$. In a similar way Hurwitz deduces that the values $f(s,a)$ for $s = -2, -3, \ldots$ are rational functions in a and m, e.g.,

$$f(-2,a) = -\frac{a(m-a)(m-2a)}{6m}.$$

In modern terms this formula is a special case of the formula

$$\zeta(-n, \tfrac{a}{m}) = -\frac{1}{n+1}B_{n+1}(\tfrac{a}{m}) \quad (= m^{-n}f(-n,a))$$

with the Bernoulli polynomials $B_k(X)$ defined by the expansion

$$\frac{t\exp(tX)}{\exp(t)-1} = \sum_{k\geq 0} B_k(X)\frac{t^n}{n!},$$

giving $B_3(X) = X^3 - \frac{3}{2}X^2 + \frac{1}{2}X$ in particular. This as well as much of Hurwitz's investigation of the functional equation in modern form can be found in Lang's books [61, 62].

Hurwitz's next aim is the proof of a functional equation for his function $f(s,a)$. For this purpose the integral J is evaluated in a second different way. In place of C where the integral was taken over a circle of radius A centered at the origin the new path is a counterclockwise oriented rectangle with vertices $(2N+1)\frac{\pi}{m}(\pm 1 \pm i)$ which includes the simple poles of the integrand at $x = \frac{2\pi i n}{m}$ with integers n such $|n| \leq N$ and excluding all others. Thus the new integral differs by the old one by the sum over all residues resulting from these poles except the one at the origin. It is no difficulty to compute the residues for $\pm n$ as

$$\frac{1}{m}\left(\frac{2\pi n}{m}\right)^{s-1} \exp(\mp\tfrac{i\pi}{2}(s-1) \mp 2\pi i\tfrac{an}{m}).$$

Now let $\operatorname{Re} s < 0$. Since then the integrals over the edges of the rectangular paths vanish as $N \to \infty$, Hurwitz arrives at the equation

$$f(s,a) = \frac{1}{\pi}\left(\frac{2\pi}{m}\right)^{s} \Gamma(1-s) \sum_{b=1}^{m}\sum_{k=0}^{\infty} (mk+b)^{s-1} \cos(\tfrac{\pi}{2}(s-1) + 2\pi\tfrac{ab}{m}).$$

Finally, after replacing s by $1-s$, this leads to the celebrated *Hurwitz formula*

$$f(1-s,a) = \frac{1}{\pi}\left(\frac{2\pi}{m}\right)^{1-s} \Gamma(s) \sum_{b=1}^{m} \cos(2\pi\tfrac{ab}{m} - \tfrac{\pi s}{2}) f(s,b). \tag{1.3}$$

By analytic continuation the latter formula holds for all values of s.

Using this powerful identity Hurwitz investigated next his main target, that is the Dirichlet series

$$F(s,D) = \sum_{n\geq 1} \left(\frac{D}{n}\right) n^{-s},$$

where $n \mapsto (\frac{D}{n})$ is the Jacobi symbol associated with a squarefree positive integer $D \equiv 1 \bmod 4$ and the summation is over all odd n coprime with D; for the cases $D \equiv 2$ or $3 \bmod 4$ a harmless factor has to be multiplied, however, for the sake of brevity we shall consider only $D \equiv 1 \bmod 4$ here. Using a decomposition of $F(s,D)$ into his functions $f(s,a)$ with $m = |D|$ and exploiting quadratic reciprocity,

Hurwitz proves that *with the only exception* $D = 1$ *the function* $F(s, D)$ *is an entire function satisfying the functional equation*

$$F(1-s, D) = \left(\frac{D}{\pi}\right)^{s-\frac{1}{2}} \frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})} F(s, D).$$

In principle, his reasoning is a simple application of the representation

$$L(s, \chi \bmod m) = \sum_{a \bmod m} \chi(a) f(s, a)$$

in combination with his identity (1.3) and explicit formulas for Gauss sums to primitive characters $\chi \bmod D$, namely

$$\sum_{a \bmod D} \chi(a) \exp\left(\frac{2\pi i a}{D}\right) = i^{\frac{1}{2}(1-\chi(-1))} D^{\frac{1}{2}},$$

which appear first by Dirichlet [18] (continuing Gauss' work [30]). Hurwitz's reasoning is actually slightly more complicated as it is nowadays presented in textbooks since the notion of primitive characters was at his time not well formulated. As a matter of fact primitive characters have been used by Edmund Landau in his 1909 monography [59]; for some reason (see 'Quellenangaben' in [59, p. 898]) his reference for that is an article by Lipschitz [69] from 1889 (more precisely he refers to pages 142–144), however, as already pointed out by Narkiewicz [77], the characters considered by Lipschitz are primitive but Lipschitz did not invent the distinction in between primitive and imprimitive characters. Whereas Hadamard did not consider the case of arithmetic progressions in his proof of the prime number theorem de la Vallée Poussin worked with characters, however, there is no notion of a primitive character in his works (since his approach does not rely on the functional equation). A Dirichlet L-function to an imprimitive character does not satisfy a functional equation of the Riemann type.

We conclude this paragraph with another quotation from the letter Hurwitz sent to Bianchi on 24 September 1881:

> My social life is very active thanks to music. I accompany my singing female friends and play with them (you don't need to think anything bad). Recently, we played eight-handed with two pianos: three women and myself. I don't know the article of Lipschitz and cannot receive it from here. From Berlin I can tell you about its contents if it is still of any value for you.[23]

Their correspondence [4] contains two further notes on this topic, the first one is a variation of Dirichlet's class number formula Hurwitz found (and reported to

[23] "Mein gesellschaftliches Leben ist durch die Musik ein sehr reges. Ich begleite meine Freundinnen zum Gesang und spiele mit Ihnen (Du brauchst nichts Schlechtes zu denken). Neulich haben wir sogar 8-händig auf 2 Claviren musicirt: 3 Damen und ich. Den Aufsatz von Lipschitz kenne ich nicht und leider kann ich mir denselben hier auch nicht verschaffen. Von Berlin aus kann ich Dir über denselben berichten, wenn es dann für Dich noch Werth hat," [4, p. 76].

Bianchi in a letter from 23 December 1881) and the second is about the delay in the publishing process (in another letter with date 20 March 1882). Not investigating what Lipschitz had done is juvenile omission. In the following we shall consider the contributions made by Lipschitz and some other contemporaries.

1.3 Aftermath and Further Generalizations by Lipschitz, Lerch, and Epstein

Rudolf Lipschitz was a student of Dirichlet. In 1864 he became professor in Bonn. He had been considered as one of the leading analysts of his time. In his first note on Dirichlet series [68] (and one of the first of all his papers) from 1857 Lipschitz studied the real and imaginary part of the $\zeta(s)$ defining Dirichlet series and generalizations thereof, namely

$$\sum_{n=-\infty}^{+\infty} \exp(2\pi\sqrt{-1}v)((n+u)\sqrt{-1}+k)^{-\sigma};$$

he obtained integral representations and identities for these infinite series. Here σ is assumed to be a real variable; in that sense Lipschitz gave birth to the funny mixture of writing $s = \sigma + it$ with Greek and Latin characters for the complex variable (which is often attributed to Landau; the imaginary part t stems from Riemann's paper), only the use of the letter "i" for the imaginary unit $\sqrt{-1}$ cannot be found in his papers. With his second article [69] from 1889 Lipschitz succeeded to give a more or less complete account of Dirichlet L-functions within an analysis of a more general Dirichlet series. Following Riemann's first proof, Lipschitz [69] obtained the identity

$$\Gamma\left(\frac{1-s}{2}\right)\sum_{n=-\infty}^{+\infty}\frac{\exp(-2\pi iv(n+u))}{((n+u)^2\pi)^{\frac{s}{2}}} = \Gamma\left(\frac{s}{2}\right)\sum_{n=-\infty}^{+\infty}\frac{\exp(2\pi inu)}{((n+v)^2\pi)^{\frac{1-s}{2}}},$$

valid for $\operatorname{Re} s \in (0,1)$. Using Gauss sums, he deduced the functional equation for quite a few Dirichlet L-functions; his reasoning is rather general. Later, Vallée Poussin [17] found another simplified proof for the functional equation of Dirichlet L-functions; the method of proof relies on Riemann's second proof of the functional equation for $\zeta(s)$. For this purpose Vallée Poussin proved a character version of the Jacobi theta-function transformation formula. His proof became standard, appearing first in Landau's *Handbuch* [59] (see also Davenport [13]).

Besides Hurwitz, Lipschitz gave credit to Mathias Lerch[24] [65] who studied two years earlier the infinite series which is nowadays well known as the Lerch zeta-

[24]Or *Matyáš Lerch* in Czech; Lerch started school only at the age of 9 years because of a severe injury of his left leg, a handicap he suffered for the rest of his life. For details of his unfortunate career and difficult character we refer to Porubský [92].

function, namely (in modern standard notation)

$$L(\lambda, \alpha, s) = \sum_{m \geq 0} \exp(2\pi i \lambda m)(m + \alpha)^{-s}$$

with real λ and α (so that $L(1, \alpha, s) = \zeta(s, \alpha)$ with $\alpha \in (0, 1]$). For this function Lerch obtained analytic continuation to the whole complex plane except a simple pole at $s = 1$ in the case of integral λ and he derived a functional identity of the form

$$L(\lambda, \alpha, 1 - s) = (2\pi)^{-s} \Gamma(s)(\exp(\tfrac{\pi i s}{2} - 2\pi i \alpha \lambda) L(-\alpha, \lambda, s) + \exp(-\tfrac{\pi i s}{2} + 2\pi i \alpha (1 - \lambda)) L(\alpha, 1 - \lambda, s)),$$

valid for $\lambda \in (0, 1), \alpha \in (0, 1]$, and $\operatorname{Re} s \in (0, 1)$. This formula includes the Hurwitz formula as limiting case $\lambda \to 0+$. It is interesting that Lerch even allowed complex values for λ and s. It seems that complex numbers and methods were widely accepted in Lerch's generation but less in the former. His reasoning is also based on Riemann's first approach to the functional equation. As particular case one deduces a result due to Lipschitz [68] and Kronecker [57], namely the identity

$$\sum_{m=-\infty}^{+\infty} \frac{\exp(2\pi i m \lambda)}{m - \alpha} = 2\pi i \frac{\exp(2\pi i \alpha \lambda)}{1 - \exp(\pi i \alpha \lambda)}.$$

Lerch mentioned previous works by Malmstèn [70] and Lipschitz [68]; moreover, in a later paper [66] he even called the latter series the *Lipschitz function*.[25] Malmstèn investigated the even more general series

$$\sum_{n=-\infty}^{+\infty} \frac{\exp(2\pi i n u)}{((n + u)^2 + v^2)^{\frac{s}{2}}},$$

which has some similarity with the so-called Epstein zeta-function associated with a quadratic form. As a matter of fact, already in a letter to Bianchi from 1881 Hurwitz had mentioned these series[26]:

[25] In 1889, Alfred Jonquiere [54] obtained the analogue of Hurwitz's formula for the polylogarithm, however, Lerch's result is more general.

[26] "Um aus diesen Formeln Vortheil für die Classenzahlen zu gewinnen, müsste man den entspr. Zusammenhang für die

$$\sum \left(\frac{1}{ax^2 + 2bxy + cy^2} \right)^s$$

erforschen."

Fig. 7 From *left* to *right*: Rudolf Otto Sigismund Lipschitz (1832–1903), Mathias Lerch (1860–1922), and Paul Epstein (1871–1939) who committed suicide during the Nazi time in the face of a summons by the Gestapo. For details about Epstein's life we refer to Siegel [108] and Burde et al. [8]

> In order to gain information about class numbers from these formulae one would have to investigate the corresponding relationship for
>
> $$\sum \left(\frac{1}{ax^2 + 2bxy + cy^2} \right)^s$$

This series appeared already in Dirichlet's paper [19]. A thorough analysis of such Dirichlet series associated with quadratic forms was realized by Paul Epstein in his 1903 paper [22].

In Hurwitz's Diary no. 6 with date 17 August 1889 we can find the following lines which seem to be a proposal for a letter he had probably written to Lipschitz, however, this letter seems to be lost[27]:

> Dear privy councillor! Mr Minkowski had informed me some time ago that my treatise on Dirichlet series is intimately related with your article published in the 54th issue of Crelle's journal. Unfortunately, I did not know this article while I was writing my treatise, hence I omitted to mention it. Recently, you were so kind to send me your article 'Untersuchung der Eigenschaften einer Gattung von unendlichen Reihen' touching this topic. Therefore I

[27] At least, Hurwitz is not mentioned in Scharlau's list [98] of letters Lipschitz had received from his contemporaries. There is also no correspondence between Lipschitz and Hurwitz in the latter one's estate, neither in Zurich nor in the archive of the Staats- und Universitätsbibliothek Göttingen where most of his letters are stored.

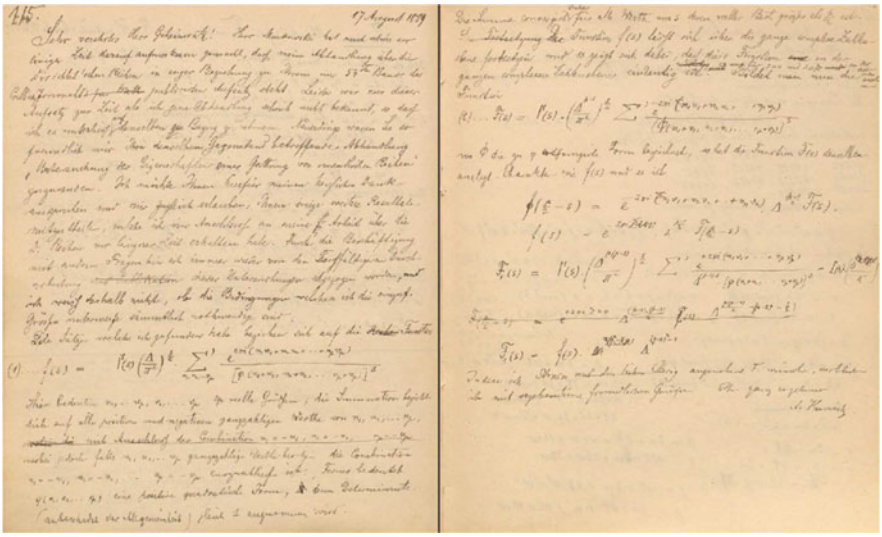


Fig. 8 The proposal for a letter to Lipschitz with date 17 August 1889, found in Hurwitz's Mathematical Diary no. 6, p. 115/116. Figures 15 and 16 show these pages in large

would like to thank you and mention a few further results which I obtained in continuation of my work about D.'s series long ago. While being occupied with further questions I was deducted from a rigorous examination of these investigations, and therefore I am not quite sure whether all conditions I suppose on the introduced objects are necessary. The theorems I have found consider the function

$$(1) \qquad f(s) = \Gamma(s)\left(\frac{\Delta}{\pi^2}\right)^{\frac{s}{2}} \sum_{n_1,n_2,\ldots n_p} \frac{e^{2\pi i(n_1v_1+n_2v_2+\ldots+n_pv_p)}}{[\varphi(n_1+u_1,n_2+u_2,\ldots n_p+u_p)]^s}$$

Here $u_1,\ldots u_p, v_1,\ldots v_p$ denote $2p$ real quantities; the summation is with respect to all positive and negative integer values $n_1,n_2,\ldots n_p$, where in case of integers $u_1,u_2,\ldots u_p$ the combination $n_1=-u_1, n_2=-u_2,\ldots n_p=-u_p$ is excluded. Moreover, $\varphi(x_1,x_2,\ldots x_p)$ stands for a positive quadratic form of (without loss of generality) determinant equal to 1. So far the sum converges for all values of s having real part greater than $\frac{p}{2}$. The function $f(s)$ can be continued over the whole complex plane and it comes out that this function is univalent and is infinite of the first kind only for $s=0$ and $s=p/2$. If we consider the function

$$(2) \qquad F(s) = \Gamma(s)\left(\frac{\Delta^{p-1}}{\pi^2}\right)^{\frac{s}{2}} \sum \frac{e^{-2\pi i(n_1u_1+n_2u_2+\ldots+n_pu_p)}}{[\phi(n_1+v_1,n_2+v_2,\ldots n_p+v_p)]^s}$$

where ϕ is the adjoint form to φ, then the function $F(s)$ has the same analytic character as $f(s)$ and

$$f(\tfrac{p}{2}-s) = e^{-2\pi i(u_1v_1+u_2v_2+\ldots+u_nv_n)}\Delta^{\frac{p-1}{2}}F(s)$$

$$f(s) = e^{-2\pi i\sum uv}\Delta^{\frac{p-1}{2}}F(\tfrac{p}{2}-s)$$

$$F_1(s) = \Gamma(s)\left(\frac{\Delta^{p(p-2)}}{\pi^2}\right)^{\frac{s}{2}} \sum \frac{e^{+2\pi i(n_1v_1+\ldots+n_pv_p)}}{\Delta^{(p-1)s}[\varphi(n_1+u_1,\ldots n_p+u_p)]^s}$$

$$F_1(s) = f(s)\Delta^{(p-2)^2-1}$$

Wishing you pleasant h. I finish with my best regards. Yours sincerely, A. Hurwitz[28]

[28]"Sehr verehrter Herr Geheimrat! Herr Minkowski hat mich schon vor einiger Zeit darauf aufmerksam gemacht, daß meine Abhandlung über die Dirichlet'schen Reihen in enger Beziehung zu Ihrem im 54 ten Bande des Crelle'schen Journals publizierten Aufsatz steht. Leider war mir dieser Aufsatz zur Zeit als ich jene Abhandlung schrieb nicht bekannt, so daß ich es unterließ auf denselben Bezug zu nehmen. Neuerdings waren Sie so freundlich mir Ihre denselben Gegenstand betreffende Abhandlung 'Untersuchung der Eigenschaften einer Gattung von unendlichen Reihen' zuzusenden. Ich möchte Ihnen hierfür meinen herzlichen Dank aussprechen und mir zugleich erlauben, Ihnen einige weitere Resultate mitzutheilen, welche ich im Anschluß an meine Arbeit über die D. Reihen vor längerer Zeit erhalten habe. Durch die Beschäftigung mit anderen Fragen bin ich immer wieder von der sorgfältigen Durcharbeitung dieser Untersuchungen abgezogen worden, und ich weiß deshalb nicht, ob die Bedingungen welchen ich die eingef. Größen unterwerfe sämtlich nothwendig sind. Die Sätze welche ich gefunden habe beziehen sich auf die Function

$$(1) \qquad f(s) = \Gamma(s)\left(\frac{\Delta}{\pi^2}\right)^{\frac{s}{2}} \sum_{n_1,n_2,\ldots n_p} \frac{e^{2\pi i(n_1v_1+n_2v_2+\ldots+n_pv_p)}}{[\varphi(n_1+u_1,n_2+u_2,\ldots n_p+u_p)]^s}$$

Hier bedeuten $u_1,\ldots u_p, v_1,\ldots v_p$ $2p$ reelle Größen; die Summation bezieht sich auf alle positiven und negativen ganzzahligen Werthe von $n_1,n_2,\ldots n_p$, wobei jedoch falls $u_1,u_2,\ldots u_p$ ganzzahlige Werthe besitzen die Combination $n_1 = -u_1, n_2 = -u_2,\ldots n_p = -u_p$ auszuschließen ist. Ferner bedeutet $\varphi(x_1,x_2,\ldots x_p)$ eine positive quadratische Form, deren Determinante (unbeschadet der Allgemeinheit) gleich 1 angenommen wird. Die Summe convergirt bisher für alle Werthe von s deren reeller Best. größer als $\frac{p}{2}$ ist. Die Function $f(s)$ läßt sich über die ganze complexe Zahlenebene fortsetzen und es zeigt sich dabei, daß diese Function in der ganzen complexen Zahlenebene eindeutig ist und nur für $s = 0$ und $s = p/2$ von der ersten Art unendlich ist. Bildet man nun die Function

$$(2) \qquad F(s) = \Gamma(s)\left(\frac{\Delta^{p-1}}{\pi^2}\right)^{\frac{s}{2}} \sum \frac{e^{-2\pi i(n_1u_1+n_2u_2+\ldots+n_pu_p)}}{[\phi(n_1+v_1,n_2+v_2,\ldots n_p+v_p)]^s}$$

wo ϕ die zu φ adjungirte Form bezeichnet, so hat die Function $F(s)$ denselben analytischen Charakter wie $f(s)$ und es ist

$$f(\tfrac{p}{2}-s) = e^{-2\pi i(u_1v_1+u_2v_2+\ldots+u_nv_n)}\Delta^{\frac{p-1}{2}}F(s)$$

$$f(s) = e^{-2\pi i\sum uv}\Delta^{\frac{p-1}{2}}F(\tfrac{p}{2}-s)$$

$$F_1(s) = \Gamma(s)\left(\frac{\Delta^{p(p-2)}}{\pi^2}\right)^{\frac{s}{2}} \sum \frac{e^{+2\pi i(n_1v_1+\ldots+n_pv_p)}}{\Delta^{(p-1)s}[\varphi(n_1+u_1,\ldots n_p+u_p)]^s}$$

$$F_1(s) = f(s)\Delta^{(p-2)^2-1}$$

Indem ich Ihnen angenehme F. wünsche, verbleibe ich mit freundlichen Grüßen. Ihr ganz ergebener A. Hurwitz" Notice that we have not copied scratched formulae or fragments of sentences. The

The analytic properties of this zeta-function were proven in Epstein's paper published in 1903 and submitted in January 1912, so 13 years after Hurwitz's letter to Lipschitz. In Epstein's paper [22] the notation

$$Z\left|\begin{matrix} g_1 \ \dots \ g_p \\ h_1 \ \dots \ h_p \end{matrix}\right|(s)_\varphi := \sum_{m=-\infty}^{+\infty} \frac{e^{2\pi i \sum_j m_j h_j}}{\varphi((g+m))^{\frac{s}{2}}}$$

is used, where $m = (m_1, \dots, m_p)$ is a tuple of integers, $g = (g_1, \dots, g_p)$ and $h = (h_1, \dots, h_p)$ are tuples of real numbers, and $\varphi((m+g))$ is the quadratic form defined by

$$\varphi((x)) = \sum_{k,\ell=1}^{p} c_{k,\ell} x_k x_\ell$$

with $c_{k,\ell} = c_{\ell,k}$ and $x = (x_1, \dots, x_p)$. Following Riemann's contour integration method, Epstein derived the following functional equation

$$\begin{aligned} &e^{2\pi i \sum_k g_k h_k} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) Z\left|\begin{matrix} g_1 \ \dots \ g_p \\ h_1 \ \dots \ h_p \end{matrix}\right|(s)_\varphi \\ &= \Delta^{-\frac{1}{2}} \pi^{\frac{s-p}{2}} \Gamma\left(\frac{p-s}{2}\right) Z\left|\begin{matrix} h_1 \ \dots \ h_p \\ -g_1 \ \dots \ -g_p \end{matrix}\right|(p-s)_\phi. \end{aligned}$$

In the easiest case, when all h_k and g_k are zero and takes the representation $\varphi((m)) = m^t Q m$ with some symmetric $p \times p$-matrix Q into account, one deduces via substituting $s \mapsto 2s$ the functional equation in the form

$$\pi^{-s} \Gamma(s) \zeta(s; Q) = (\det Q)^{-1} \pi^{s-\frac{p}{2}} \Gamma\left(\frac{p}{2} - s\right) \zeta\left(\frac{p}{2} - s, Q^{-1}\right)$$

for the Epstein zeta-function

$$\zeta(s, Q) := \sum_{0 \neq m \in \mathbb{Z}^p} (m^t Q m)^{-s}$$

as it usually appears in the recent literature. We notice that this is essentially in coincidence with Hurwitz's remark. Epstein mentioned Hurwitz's paper [46] on the Hurwitz zeta-function as well as Lipschitz [69] and Lerch [65] (but, of course, not Hurwitz's diary entry nor his lost letter to Lispchitz). Furthermore, Epstein wrote

> Consequently, for the so far most general zeta-function, investigated by Mr Lipschitz, there exists an integral representation in terms of an infinite theta series of *arbitrary* characteristic. Following this thought we define a *general zeta-function of pth order* by a p-folded infinite

abbreviation 'F.' might stand for 'Ferien' meaning 'holidays', so we have used the letter 'h.' in our translation.

> series which generalizes Riemann's zeta-function in just the same way as the general theta series of pth order generalizes the elliptic theta series. This extension of the zeta-function is natural since the above mentioned theorem of Riemann about the function $\zeta(s)$ can be transferred to the general zeta-function in a surprisingly easy way.[29]

We do not want to go into the details of the appearing notions; and we also do not explain here the different theta-functions but remark that Epstein's approach is obviously via Riemann's second proof of the functional equation (and Vallée Poussin's generalization to Dirichlet L-functions).[30]

A last comment about Hurwitz's letter to Lipschitz. In 1887, after studying with Hurwitz in Königsberg, his former pupil and friend Hermann Minkowski became professor at the University of Bonn where Lipschitz was professor (from 1864 until the end of his life in 1903). We may speculate that this contact had been a reason for the correspondence between Hurwitz and Lipschitz.[31] Bianchi's hint from his 1881 letter is not mentioned.

We conclude with a discussion about the name attributed to Hurwitz's generalization. Reading Landau's historical survey [58] from 1906, we find the Hurwitz zeta-function with notation $\zeta(s, w)$; a quotation of Hurwitz is missing, however, Mellin [71] is mentioned. In 1929, Walter Schnee [103] gave a new proof of the functional equation for $\zeta(s, \alpha)$ and Dirichlet series with periodic coefficients, however, Hurwitz is not mentioned. The same in Helmut Hasse's paper [41], where $\zeta(s, \alpha)$ is called "allgemeine ζ-Reihe." In 1950/51 this was changed by two articles in the same volume of the *Proceedings of the American Mathematical Society*, namely Fine [26] and Apostol [2]. The first paper, the one by Fine, gives a proof of the functional equation for the Hurwitz zeta-function by means of Riemann's second approach using Poisson summation and properties of Jacobi's

[29] "Dem entsprechend existirt für die von Herrn Lipschitz untersuchte Function—die allgemeinste bisher betrachtete 'Zeta'-function—eine Integraldarstellung mit Hülfe einer unendlichen Thetareihe mit *beliebiger* Charakteristik. Diesem Gedankengange folgend definiren wir als *allgemeine Zetafunction* p^{ter} *Ordnung* eine p-fach unendliche Reihe, welche in gleicher Weise eine Verallgemeinerung der Riemann'schen ζ-function darstellt, wie die allgemeine Thetareihe p^{ter} Ordnung gegenüber der elliptischen Thetareihe. Dass diese Erweiterung der Zetafunctionen naturgemäss ist, zeigt sich vor allem darin, dass sich der oben angeführte Riemann'sche Satz über die Function $\zeta(s)$ in überraschend einfacher Weise auf die allgemeinste Zetafunction übertragen lässt." [22, p. 616].

[30] In a subsequent paper the authors intend to investigate the Hurwitz estate further in order to find details about his approach to zeta-functions associated with quadratic forms.

[31] In 1897, Minkowski married Auguste Adler from Strasbourg, the place where Epstein obtained his doctorate in 1895 (advised by Elwin Christoffel) and remained as docent until 1919 when he received the call of the recently founded university in his native town of Frankfurt/Main. As a matter of fact, Minkowski was frequently visiting his brother and famous physician Oskar at Strasbourg starting from 1889 as we know from Hermann Minkowski's letters to Hilbert [75]; during some of these visits Minkowski got in touch with the mathematicians at Strasbourg University and Christoffel in particular (see [75, p. 34 and 36]). A word about Frankfurt University, too. This institution was founded in 1914, mainly by donations of the Jewish community of Frankfurt, but the Jew Epstein was driven to commit suicide under the Nazi regime. Actually, all members of the Frankfurt Mathematical Seminar except Siegel lost their positions.

theta-function. The second paper, the one by Apostol, gives another proof relying on Lerch's transformation formula. Both authors explicitly call $\zeta(s, \alpha)$ the Hurwitz zeta-function. We do not consider the many further research papers on the Hurwitz zeta-function here. The name Epstein zeta-function for the generalization associated with quadratic forms, however, has been used since Edward Charles Titchmarsh's article [110] from 1934.

The Hurwitz zeta-function $\zeta(s, \alpha)$ with an irrational parameter α is not treated in Hurwitz's original paper. For example, in the monographs of Lang [61, 62] and Garunkštis and Laurinčikas [29] the reader may find (essentially the same) proof for the Hurwitz zeta-function with a not necessarily rational parameter and in the latter one the proof of the functional equation for the more general Lerch zeta-function.

Obviously, some of the mathematicians mentioned above were not very well informed about what others did. The standards of citation were rather different in the nineteenth century, and so the distribution of research results and of journals as well. Another aspect is that it was not quite clear in the process of generalization from the Riemann zeta-function and Dirichlet L-series which one of all the various possible generalized zeta-functions would be the best (if one really would like to coin the notion "best" in this context). The struggle for the *best* generalization of the Riemann zeta-function reminds the authors on the numerous approaches to multiple (multivariate) zeta-functions and zeta-values in the literature (e.g., the Euler-Zagier multiple zeta-functions) investigated intensively for about 25 years.

2 Königsberg and Zurich: Entire Functions

In 1884 Adolf Hurwitz became extraordinary professor at the University of Königsberg (now Kaliningrad in Russia) on invitation of Ferdinand Lindemann. Although friends and relatives as well as most of his former mathematical friends and colleagues were far distant Hurwitz spent a very good time in Königsberg. He produced many beautiful theorems and he was rather successful in teaching: among the few Königsberg students Hurwitz had with David Hilbert and Hermann Minkowski two brilliant pupils. During frequent walks Hurwitz introduced the two students to various mathematical disciplines and guided their first steps in research. The three of them became lifelong friends. Moreover, Adolf Hurwitz got to know his later wife, Ida Samuel, the daughter of the professor for Pathology at Königsberg University; they married in summer 1892. In the same year Frobenius left Zurich for Berlin and Hurwitz was offered the vacant ordinary professorship. The young family moved to Switzerland.

Fig. 9 Ida Samuel-Hurwitz (1864–1951) and Adolf Hurwitz; the photograph has been taken in the Königsberg period, probably around the time of their marriage in 1892

2.1 Prehistory: The Proof of the Prime Number Theorem

Riemann's celebrated paper [93] is at least nowadays considered most important with respect to its not rigorously proved statements and conjectures. This memoir has indeed been a signpost for developing complex analytic methods in order to reveal distribution properties of the prime numbers. Taking Riemann's personality into account one may understand his contribution also as an outline of a far reaching analytic method in number theory, leaving the details to the posterity. The announced product representation was obtained by Jacques Hadamard [35] in 1893, the explicit formula linking the zeros of $\zeta(s)$ with the prime numbers was proved by von Mangoldt [111] in 1895, the so-called Riemann-von Mangoldt formula for the number of zeros inside certain rectangles was as well obtained by von Mangoldt in the same paper; only the famous Riemann hypothesis claiming that all nontrivial zeros lie on the critical line has remained unsolved until today.[32] Building

[32] Actually, Riemann wrote that it is "very likely" that all these zeros lie on a line; he did neither announce this comparable to his other claims nor did he formulate it as a conjecture. Nowadays

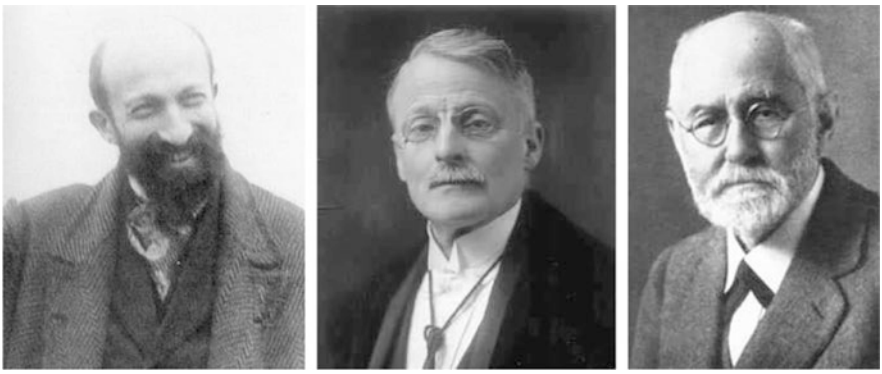


Fig. 10 On the *left* Jacques Hadamard (1865–1963); together with Émile Zola and others he was supporting Alfred Dreyfus in the Dreyfus affair in the 1890s. In the *middle* Charles Jean Gustave Nicolas Baron de la Vallée Poussin (1866–1962). It is legend that everyone who provides a new proof of the prime number theorem is immortal; Hadamard and Vallée Poussin died at age almost 100 years. On the *right-hand side* Hans von Mangoldt (1854–1925) who served as rector for the *Königliche Technische Hochschule Aachen* (now *RWTH Aachen*) for 1899–1901. His contributions became major tools in zeta-function theory

on Riemann's ideas, Hadamard [37] and Charles de la Vallée Poussin [16] solved in 1896 independently a conjecture of Gauss on the number of primes below a given magnitude; their reasoning culminated in the celebrated prime number theorem giving the asymptotics for the counting function $\pi(x)$ of prime numbers $p \le x$, namely

$$\lim_{x\to\infty} \pi(x)\frac{\log x}{x} = 1\,, \qquad \text{resp.} \qquad \pi(x) \sim \frac{x}{\log x}$$

as $x \to \infty$. More precise formulae provide explicit error terms depending on the zero-free region for the zeta-function. For details on the history of the development of the prime number theory we refer to Narkiewicz's monumental [77], Laugwitz's Riemann biography [63], and Schwarz's survey [104].

2.2 *Hadamard's Theory of Entire Functions of Finite Order*

A function $f(s)$ is called entire if it is analytic (holomorphic) throughout the whole complex plane; if its absolute value is not growing too quickly as $|s|$ tends to infinity, it is said to be of finite order (and "of finite genre" in older literature). Since the Riemann zeta-function $\zeta(s)$ is analytic except for a simple pole at $s = 1$, it is natural to consider $(s-1)\zeta(s)$ or similar functions with respect to the general theory of

we can only speculate whether Riemann knew about the arithmetical consequences of such a zero distribution.

entire functions. This line of inquiry had been established among others by Jacques Hadamard in his dissertation [34] from 1892 advised by Émile Picard. Hadamard's motivation, however, was not the theory itself but its application to the unsolved problems around the Riemann zeta-function. In fact, his theory of entire functions of finite order constitutes a major ingredient in his and de la Vallée Poussin's celebrated proof of the prime number theorem and later refinements.

In the *Jahrbuch der Mathematik* we can read in a review by Adolf Hurwitz concerning Hadamard's article [35]:

> The article under review is the accomplishment of a work which had been awarded the great mathematical prize of the Parisian Academy of Sciences. Taking into account that the author had only a limited amount of time, it is attributed that the formulation of the article causes trouble to its comprehension. For example, the proof of the main theorem from the first part should have been arranged differently in order to be rigorous. This is just about the outward appearance of the work; as regards content it may be considered as one of the most important function-theoretical pieces of the last years.[33]

Indeed, Hadamard's article under consideration had been awarded the *Grand Prix des Sciences Mathématique* of the French Academy of Sciences in 1892 for a treatise on the Riemann zeta-function (reporting about the results from his doctorate). Hurwitz wrote several hundreds of reviews of articles in German, French, Italian, and English for the *Jahrbuch über die Fortschritte der Mathematik*[34] and these reviews provide a mathematical fingerprint of his research activities and interests. Hurwitz followed the many works dealing with entire functions in particular and his diaries contain numerous entries about this topic. In his Mathematical Diary No. 15, we find for 22 February 1897 an entry analyzing the Hadamard's papers [36, 37] on the distribution of zeros of $\zeta(s)$ and its arithmetical consequences. It is interesting to notice that Hadamard cited Hurwitz's paper [46] (besides Cahen [9]) and made use of his identity.

2.3 Pólya and Hurwitz's Estate

George (György) Pólya was born in Budapest 1887; he finished his studies in 1912 with a doctorate supervised by Lipót Fejér in Budapest, investigating

[33] "Die vorliegende Abhandlung ist die weitere Ausführung einer Arbeit, die von der Akademie der Wissenschaften zu Paris mit dem grossen mathematischen Preise gekrönt worden ist. Dem Umstande, dass der Verfasser nur eine beschränkte Zeit zur Verfügung hatte, ist es wohl zuzuschreiben, dass die Abfassung der Abhandlung dem Verständnisse manche Schwierigkeiten bereitet. So muss beispielsweise der Beweis des Hauptsatzes im ersten Teile der Arbeit anders angeordnet werden, um bindende Kraft zu erhalten. Diese Ausstellung betrifft indessen nur die äussere Form der Arbeit; inhaltlich darf dieselbe wohl als eine der bedeutendsten functionentheoretischen Arbeiten der letzten Jahre bezeichnet werden."

[34] Which was founded as early as 1868 by Carl Orthmann and Felix Müller and served as prerunner of Mathematical Reviews and Zentralblatt until 1942; now its many reviews are included into the Zentralblatt data bank.

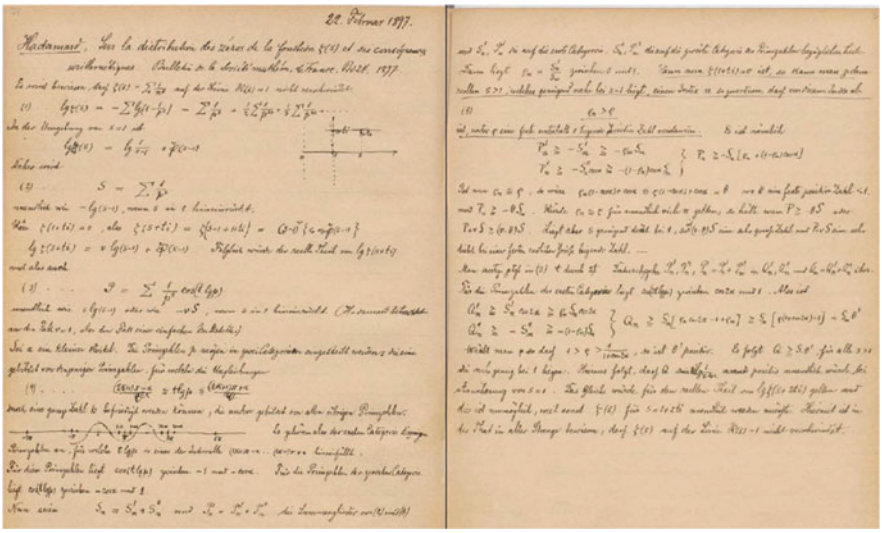


Fig. 11 In Hurwitz's Mathematical Diary no. 15, 22 February 1897, p. 38/39, one can find detailed notes about Hadamard's reasoning for proving the non-vanishing of $\zeta(1+it)$ for real t from his 1896 paper [37] which is equivalent to the prime number theorem as was first proved by Landau and used in his proof of the prime ideal theorem [58] in 1903. Interestingly, also Diary no. 11 contains a few notes on the pages 52–66 about the same article [37] similar to the one in Diary no. 15 from above. They appear without date; in fact Diary no. 11 was started in 3 October 1894 but never finished

geometric probability. After a postdoc in Göttingen he started at the Eidgenössische Hochschule Zurich in 1914 on promotion by Hurwitz. He became extraordinary professor in 1920 and ordinary professor only in 1928 (despite his numerous important results).[35] In 1940 Pólya moved to the USA where he had professorships at several universities, since 1942 in Stanford. Pólya died in Palo Alto in 1985. He is considered as one of the outstanding mathematicians of the twentieth century. As his mentor and colleague Hurwitz Pólya had a broad mathematical knowledge and interest.

> He also credited Hurwitz's extensive mathematical diaries for a number of problems that later appeared in the *Aufgaben und Lehrsätze*. These diaries may have influenced Pólya in other ways: he kept a mathematical log himself throughout much of his career, recording mathematical conversations and keeping track of his own mathematical ideas.

wrote Alexanderson and Lange [1]. The mentioned book *Aufgaben und Lehrsätze aus der Analysis* was a joint work with Gabor Szegő and the innovative style of this collection of exercises (ordered with respect to methods to prove these results rather

[35]The Lerch pupil Michel Plancherel was chosen to inherit Hurwitz's chair, not Pólya although he was considered as outstanding mathematician by none less than Hilbert and Hadamard; see Frei and Stammbach [27, p. 51] for details.

Fig. 12 On the *left*: George Pólya (1887–1985) who also kept a mathematical diary. In the *middle*: Johan Ludwig Valdemar Jensen (1859–1925) who did not keep a mathematical diary. On the *right* another photograph of Adolf Hurwitz about the time when he got to know Pólya

than the results itself) is still a pearl in the mathematical literature. Besides many interesting tasks it includes, for example, the proof of the existence of infinitely many prime numbers by use of the coprimality of the Fermat numbers $2^{2^n}+1$ which is probably based on lectures of Hurwitz' which were later published as [50][36] and the letter exchange between Goldbach and Euler; for details we refer to Haas [33].

Starting in 1921, two years after Adolf Hurwitz's death in Zurich 18 November 1919, Pólya became literary executor of Hurwitz's estate. In 1933 Hurwitz's collected papers were finally published, edited by Pólya. The mathematical diaries of Adolf Hurwitz definitely had been another source of inspiration for Pólya.[37] Here we shall focus on zeta-function theory.

> Of those topics which are treated in the diaries for several years again and again we shall mention here Riemann's zeta-function as an example; in the published works of Hurwitz this object is not mentioned at all. Very early Hurwitz had tried a path towards the Riemann hypothesis in vain which some years later also Jensen found: (...) The aim was unreachable.[38]

These words are due to George Pólya introducing and commenting the unpublished notes of Adolf Hurwitz [90, p. 6]. The first mathematical diary started in 25 April 1882, too late for Hurwitz's work on the Hurwitz zeta-function [46].

[36] And may have been also an inspiration for the book [91] of Pólya & Szegö.

[37] Since in Hurwitz's last diary one can find some notes from 1918 about Arthur Cayley's studies of counting trees, namely alkane C_nH_{2n+2} with certain restrictions, one could speculate whether this might have been an inspiration for Pólyas celebrated enumeration theory.

[38] "Von denjenigen Gegenständen, auf welche die Tagebücher lange Jahre hindurch immer wieder und wieder zurückkommen, sei hier als Beispiel nur die Riemann'sche ζ-Funktion hervorgehoben; in den veröffentlichten Arbeiten von Hurwitz wird dieser Gegenstand wohl nicht einmal erwähnt. Schon früh hat Hurwitz den Weg zur Riemann'schen Vermutung versucht, den einige Jahre später auch Jensen, ebenfalls ergebnislos versucht hat: (...) Das Ziel war unerreichbar."

> Hurwitz was the type of mathematician who always achieved something when seriously using his power, if not the envisaged objective, then at least something interesting besides. Two side issues of his efforts about the ζ-function reached the mathematical community by oral communication:...[39]

This quotation is again from Pólya's introductory words to Hurwitz's estate [90], p.7. Indeed Pólya himself had continued some of Hurwitz's ideas.

In 1914, Godfrey Harold Hardy [40] proved that infinitely many zeros of $\zeta(s)$ lie on the critical line. His reasoning was based on the real-valued function defined essentially by the left-hand side of the functional equation, i.e.,

$$\Xi(t) := \tfrac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s)|_{s=\frac{1}{2}+it}$$

and its integral representation

$$\Xi(t) = \tfrac{1}{2} - (t^2+\tfrac{1}{4})\int_1^\infty x^{-\frac{3}{4}}\cos(\tfrac{1}{2}t\log x)\sum_{n\geq 1}\exp(-\pi n^2 x)\mathrm{d}x.$$

Hardy's reasoning relies on the integral

$$\int_0^\infty \Xi(t)\frac{t^{2n}}{t^2+\frac{1}{4}}\cosh(\alpha t)\mathrm{d}t$$

and taking the limit $\alpha \to \frac{\pi}{4}-$ under the assumption that $\Xi(t)$ is of constant sign for all sufficiently large t. By the upcoming contradictions it follows that $\Xi(t)$ must have infinitely many odd order zeros, and since all factors of $\Xi(t)$ do not vanish except $\zeta(\frac{1}{2}+it)$ possibly, this proves the existence of infinitely many zeta zeros on the critical line. In Hurwitz's Mathematical Diary no. 26 we can find an outline of Hardy's proof. Pólya [87] found a variant of Hardy's proof by the associated Fourier integral

$$\Phi(u) := \tfrac{1}{\pi}\int_0^\infty \Xi(t)\cos(ut)\mathrm{d}t$$

and its Taylor expansion. The same line of inquiry has been treated by Pólya in his papers [85, 86, 88]. Probably, the easiest proof of Hardy's theorem is due to Landau [60, p. 78], which relies on the inequality

$$\int_T^{2T} Z(t)\mathrm{d}t < \int_T^{2T} |Z(t)|\mathrm{d}t,$$

[39] "Nun war Hurwitz von dem Mathematikertypus, der bei ernstlicher Einsetzung seiner Kräfte immer etwas erreicht, wenn nicht das ursprünglich ins Auge gefasste Ziel, so doch etwas Interessantes auf den Seitenwegen. Zwei Nebenresultate seiner Bemühungen um die ζ-Funktion sind durch mündliche Mitteilungen in die mathematische Oeffentlichkeit gelangt: ...".

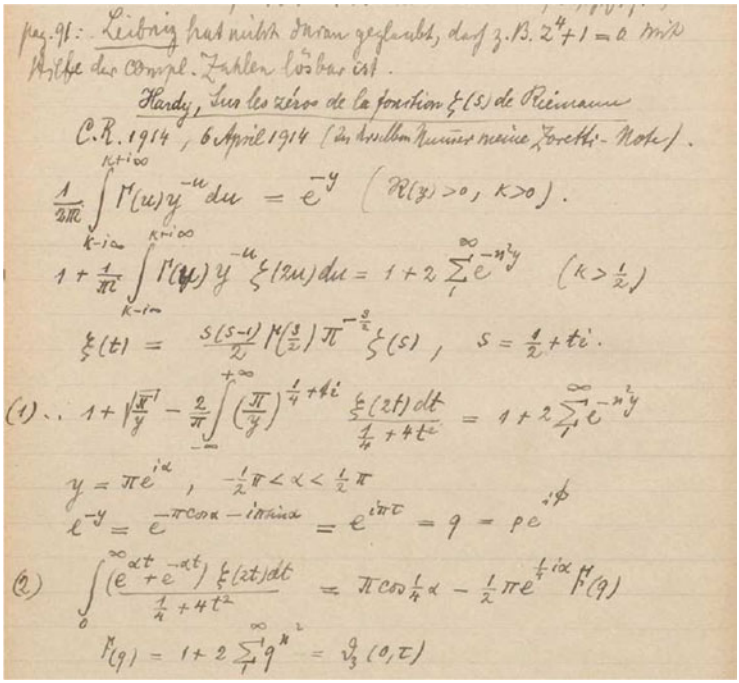


Fig. 13 Hurwitz's notes of Hardy's proof from his Diary no. 26, p. 181. Hurwitz noticed that Hardy's article had been published in the same issue as one of his papers [49] correcting an inaccuracy in Ludovic Zoretti's book *Leçons sur le prolongement analytique* from 1911. The sentence on top claims that Leibniz did not believe that the equation $z^4 + 1 = 0$ could be solved using complex numbers

valid for sufficiently large T, where

$$Z(t) := \exp(i\theta(t))\zeta(\tfrac{1}{2} + it)$$

with

$$\exp(i\theta(t)) := \pi^{-\frac{it}{2}} \frac{\Gamma(\frac{1}{4} + \frac{it}{2})}{|\Gamma(\frac{1}{4} + \frac{it}{2})|}$$

is real-valued. Hardy's approach allows quantitative results, however, the so far best quantitative bound for the number of zeros on the critical line was obtained by Levinson's method and its technical refinements.[40]

Pólya's paper [84] from 1918 deals with the zeros of entire functions represented by certain Fourier integrals. It even contains a theorem due to Hurwitz and his proof

[40] See Iwaniec [52] for a recent presentation.

(see [84, p. 368]), namely: *given an even function $f(t)$ defined for $t \in (-1, 1)$ having alternating Fourier coefficients, i.e.,*

$$f(t) \sim \tfrac{1}{2}a_0 + a_1 \cos(\pi t) + a_2 \cos(2\pi t) + a_3 \cos(3\pi t) + \ldots$$

with $a_0 > 0, a_1 < 0, a_2 > 0, a_3 < 0, \ldots$, then the zeros of the entire function

$$U(z) = \int_0^1 f(t) \cos(zt) \mathrm{d}t \tag{2.1}$$

are all real and simple, and such that in each of the intervals $\ldots, (-2\pi, -\pi)$, $(-\pi, 0)$, $(0, \pi), (\pi, 2\pi), \ldots$ contains exactly one zero. This result and its rather lengthy proof is related to Pólya's reasoning; moreover, a paper of Jensen is mentioned. And the name Jensen comes up in another context as well. For his article [87] Pólya has studied the mathematical papers left by Johan Ludwig William Valdemar Jensen.[41] The autodidact Jensen never had an academic appointment, however, working for the International Bell Telephone Company at Copenhagen, he found time for severe mathematical research. In zeta-function theory the so-called Jensen formula plays an important role in estimating the number of zeros of an entire function in a given disk.[42] In 1911, during the Second Congress of Scandinavian Mathematicians at Copenhagen Jensen [53] announced five articles about new algebraic and function-theoretical methods with applications to the Riemann zeta-function (JV), however, none of these announcements was published until Jensen's death in 1925. Probably inspired by his studies of Hurwitz's estate, Pólya investigated the Jensen estate (JN) but could not find what he was aiming at.

> This all is to find in several small notebooks and a great number of loose pages such that in most cases it is impossible to fix in which sequence and which time the notes have been written down. As follows from this description the state of the estate does not allow to set its content with certainty.[43]

It seems that Jensen was in some sense a messy mathematician as Hurwitz was a tidy character. This chaos did not stop Pólya's investigations; he even wrote a survey on integral representations and their applications with respect to the Riemann zeta-function. In this context Pólya gave credit to Hurwitz:

> I is contained in JV (p. 188), II and III are often quoted in JN. For II and IV see P_3. II and III were (as well as the consequences mentioned in Nr. 6 following Theorem III) known

[41] It is interesting to notice that around the same time Carl Ludwig Siegel was investigating Riemann's estate in Göttingen; his study [106] has changed the impression many contemporaries had about Riemann's approach to number theory.

[42] According to Narkiewicz [77], p. 258, Jensen's formula was essentially known by Carl Gustav Jacobi already in 1827.

[43] "Dies alles in einigen kleinen Heften und an einer grossen Anzahl von losen Blättern, so dass in den allermeisten Fällen unmöglich festzustellen ist, in welcher Reihenfolge und zu welchem Datum die Aufzeichnungen entstanden sind. Wie aus dieser Schilderung hervorgeht, erlaubt der Zustand des Nachlasses nicht, dessen Inhalt mit Sicherheit festzustellen."

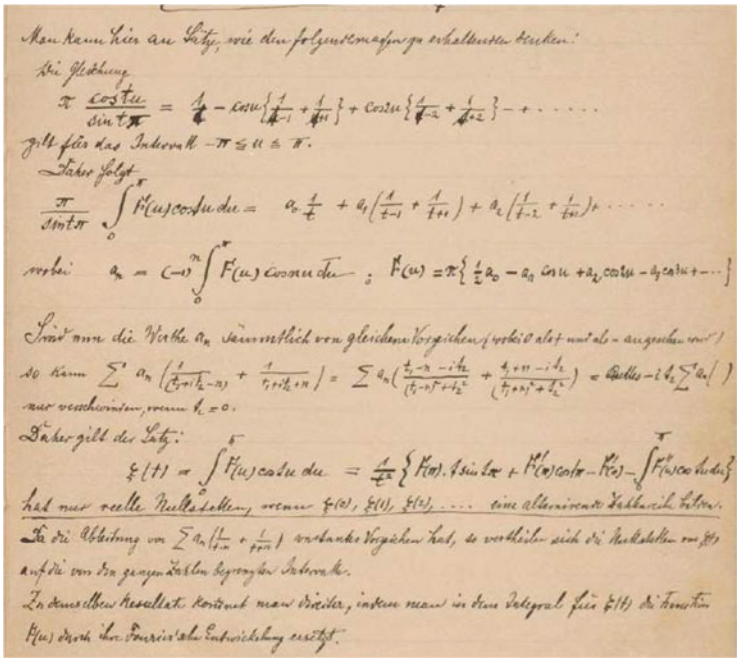


Fig. 14 Hurwitz's Diary no. 17, p. 115. Formula (2.1) appears in disguised form in the lower third. Another entry of the diary, a few pages later, bears the date 3 December 1899

by several friendly mathematicians; both appear in the mathematical diaries of A. Hurwitz (preserved by the library of the Eidg. Technischen Hochschule in Zurich) with date 1899.[44]

Indeed, in the Mathematical Diary no. 17, pp. 112–115, we can find the corresponding formula (see Fig. 14).

Now we are in the position to explain what Pólya meant in writing "Very early Hurwitz had tried a path towards the Riemann hypothesis in vain which some years later also Jensen found" (as mentioned above). In 1889, Hurwitz [47] extended a classical result due to Siméon Poisson [81, p. 178], on the zeros of Bessel functions J_n (whose definition we omit here), namely that all the zeros are real when $n \geq 1$. He extended and quantified Poisson's result about the zero-distribution using Rouché's theorem[45] and more advanced techniques; in particular he obtained his famous

[44] "I ist in JV (S. 188), II und III sind in JN öfters hervorgehoben. Für II und IV vgl. P_3. II und III waren (nebst der in Nr. 6 im Anschluss an Satz III hervorgehobenen Konsequenzen) mehreren mit mir befreundeten Mathematikern bekannt; beide kommen in den Tagebüchern von A. Hurwitz (aufbewahrt in der Bibliothek der Eidg. Technischen Hochschule in Zürich) unter dem Datum 1899 vor," [87, p. 11]. Here P_3 is an abbreviation for [85].

[45] Which probably was unknown to him and better should be named after Augustin Louis Cauchy as already Eugène Rouché had remarked; see Bottazini and Gray [7] for details.

theorem on *uniformly convergent sequences of meromorphic functions having limit either identically vanishing or*, more interestingly, *every zero of the limit function is limit of the zeros of the functions in the sequence*. This result is now a standard tool in the complex analytic tool box. Using this observation, Hurwitz was led to a separation of the real zeros as in the case of (2.1) above. And here is the link to his approach to the Riemann hypothesis. Hurwitz wrote:

> The proof of this theorem is, following Poisson's process, usually based on an integral representation...[46]

We observe the similarity with the situation considered by Hardy and the entry in Diary no. 17 (Fig. 14) from above. In order to prove that all nontrivial zeros of the zeta-function are on the critical line one could aim at finding a suitable integral representation; this could be realized by giving criteria that an entire function (e.g., a Fourier transform of a kernel) has all its zeros on the real axis. This idea appears in the literature several times; however, it seems that Hurwitz was among the first to have considered this approach "in vain (...) the aim was unreachable" as Pólya remarked.

In a subsequent paper [88], following an idea of Landau, Pólya obtained the related remarkable result that all zeros of the function

$$\Xi^*(t) := 4\pi^2 \int_0^\infty \cosh(\tfrac{9}{2}u) \exp(-2\pi \cosh(2u)) \cos(ut) \mathrm{d}t$$

are real; although this function is an approximation of $\Xi(t)$, unfortunately this has no impact on the location of the zeros of the Riemann zeta-function. Nevertheless it reminds us of another related approach to the Riemann hypothesis. Based on a theorem due to Edmond Nicolas Laguerre on entire functions with real zeros, Pólya [82] studied sequences of polynomials with positive real roots and proved that a uniform limit is either vanishing identically or an entire function of order zero or one (see (2.2) below). Interestingly, Pólya's paper includes a certain criticism of Laguerre's proof:

> The correctness of this proof can be doubted; I am of the opinion that the proof can be realized rigorously without any substantial changes. The here given proof is completely independent of the correctness of Laguerre's reasoning.[47]

It should be mentioned that [82] had been written in 1913, Pólya's last year in Göttingen before he moved to Zurich. Around the same time Jakob Grommer wrote his doctorate [32] supervised by Hilbert on this topic. He found an improvement of one of Hurwitz's unpublished theorems on entire functions with real zeros only; the

[46] "Der Beweis dieses Satzes pflegt man nach Poisson's Vorgang auf eine Integralformel zu gründen..."; [47, p. 246].

[47] "Die Richtigkeit dieses Beweises kann angezweifelt werden; ich bin der Ansicht, dass der Beweis ohne wesentliche Aenderungen des Gedankenganges lückenlos zu führen ist. Der hier gegebene Beweis ist von der Richtigkeit des Laguerreschen völlig unabhängig, und beruht auf einer ganz anderen Grundlage.", [82, p. 280].

original result and questions about its possible generalization were communicated by Otto Toeplitz and it was Hilbert who supported Grommer "who apart from his physical ailment faced triple jeopardy as a foreigner, orthodox Jew, and as someone without the equivalent of the *Abitur*, since he graduaded from a Talmudic school rather than a traditional Gymnasium" wrote Rowe and Schulmann [95]. Grommer's thesis forms the second issue Pólya had mentioned in his comment about the Hurwitz estate.

It seems that these kind of questions were among the first that Hurwitz and Pólya discussed after the latter's arrival at Zurich in 1913. In Diary no. 26 one can find an entry on "Pólya's theorem" under date 26 February 1914 which is related to his publication [83]; actually, the same diary contains a note with respect to Laguerre's theorem as well as an application of Charles Biehler's theorem [5] on real zeros of entire functions with comment

> A pretty application of Biehler's theorem came to me last night.[48]

In the recent literature the so-called Laguerre–Pólya class is defined as the set of entire functions $E(s)$ being locally limits of a series of polynomials having only real roots. Such functions obey (like polynomials) the Hadamard product representation

$$E(s) = s^d \exp(a + bs + cs^2) \prod_n \left(1 - \frac{s}{s_n}\right) \exp\left(\frac{s}{s_n}\right), \tag{2.2}$$

where a, b, c are constant, b and c real, the latter one zero or negative, d is the multiplicity of a (hypothetical) zero at $s = 0$, and the s_n denote the further zeros of E. There is a lot of literature on this class of entire functions and their zero-distribution; the impact on the Riemann zeta-function and allied functions has been investigated for decades, e.g., Louis de Branges [15] should be mentioned here. However, since this is not really related to Adolf Hurwitz and his mathematics, we refer here only to the survey article [12] by Csordas, Norfolk and Varga. In particular Pólya's paper [82] has been extended and precised by Dennis Hejhal [45].

Another idea in the context of the Riemann hypothesis related to Pólya is the so-called Hilbert-Pólya conjecture that the ordinates of the nontrivial zeros of the Riemann zeta-function correspond to eigenvalues of an unbounded self-adjoint operator. This idea as well does not go back to conversations with Hurwitz but arose from Pólya's time in Göttingen and a question by Landau.[49]

3 Concluding Remarks

Introducing analytic methods to number theory was a change of paradigm. The ideas of Euler, Dirichlet, and Riemann, however, were ahead the methods at their time. Open question about prime number distribution became a driving force for

[48] "Eine hübsche Anwendung des Biehler'schen Satzes fiel mir vergangene Nacht ein."

[49] See the correspondence [89] between Andrew Odlyzko and Pólya on this topic.

the development of certain aspects of complex analysis. The distribution of zeros of zeta- and L-functions is still not understood very well. This might have two reasons: it is neither known what impact a Riemann type-functional equation on the zeros distribution actually has nor is it clear why arithmetically relevant Dirichlet series with an Euler product seem to have all its complex zeros on one single line.[50] The functional equation alone cannot be the driving force for the complex zeros to lie on the critical line. Harold Davenport and Hans Heilbronn [14] showed that the Hurwitz zeta-function $\zeta(s,\alpha)$ has infinitely many zeros in the half-plane $\operatorname{Re} s > 1$ provided $\alpha \neq \frac{1}{2}, 1$ is rational or transcendental; moreover, they showed the explicit existence of Dirichlet series satisfying a Riemann-type functional equation having infinitely many zeros off the critical line. It is expected that the Euler product should have a severe impact on the zero-distribution (although there is no absolute convergence of the Euler product inside the critical strip).

The second proof Riemann gave for the functional equation of the zeta-function may be considered more important by its relation to modular forms. This line of investigation has been studied by Erich Hecke starting with his proof of the functional equation for Dedekind zeta-functions [43] in 1916/17 and the relation between Dirichlet series having a functional equation of the Riemann type and modular forms [44] in 1936. Nowadays the role of Dirichlet series for arithmetical questions is quite fairly understood. We quote

> In recent years L-functions and their analytic properties have assumed a central role in number theory and automorphic forms.

from the abstract of Gelbart and Miller [31] which gives an excellent reading for the modern zeta-function theory. We shall briefly mention here John Tate's thesis [109] in which a proof of the functional equation is given on the basis of local methods. This method can be interpreted as an analytic variation of the local global principle discovered by Helmut Hasse for quadratic forms. Another line of inquiry has been suggested by Robert P. Langlands in the 1970s with his "Langlands Program" claiming that all arithmetically relevant L-functions (automorphic or motivic) arise as products of L-functions associated with automorphic representations; the celebrated proof of the Shimura and Taniyama conjecture due to Andrew Wiles et al. is a prominent example. For details we refer once again to [31]. On the contrary, the first proof Riemann gave in his path-breaking paper and Hurwitz's generalization still gives (at least in the authors' opinion) the most simple approach to Dirichlet L-functions (without using Poisson's summation formula).

We summarize. Shortly after receiving his doctorate in 1881 Adolf Hurwitz made new contacts and found research problems in new mathematical topics. One of them, zeta-function theory, should be a field of interest for the rest of his life although this is apart from his paper on the Hurwitz zeta-function not visible in his list of publications. His mathematical diaries and a few reviews as well as the remarks in

[50] Actually, the notion of an L-function is usually used for zeta-functions having an Euler product. An axiomatic setting for such arithmetically relevant Dirichlet series was provided by Atle Selberg [105]. It is legend that the letter "L" is chosen with respect to Dirichlet's given name "Leujene."

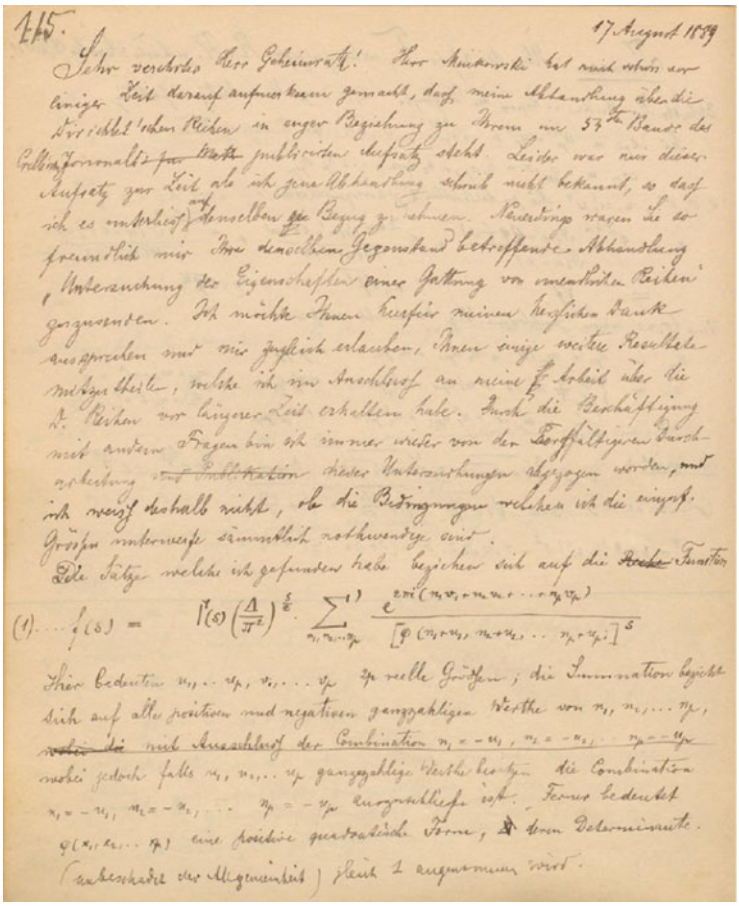


Fig. 15 Page 115 from the mathematical Diary no. 6, [51]

Pólya's papers, however, give proof for this liking. Hurwitz's ideas concerning the Riemann zeta-function and its relatives have inspired many contemporaries and later mathematicians and traces can be found until today. Last not least, Hurwitz was in possession of fundamental insights about an important generalization of the variety of zeta-functions under investigation at the turn of the century. Unfortunately, he (probably) only communicated his results about these zeta-function to quadratic forms in a letter to Lipschitz but did not find time to polish and publish his notes; nowadays all the credit is given to Epstein.

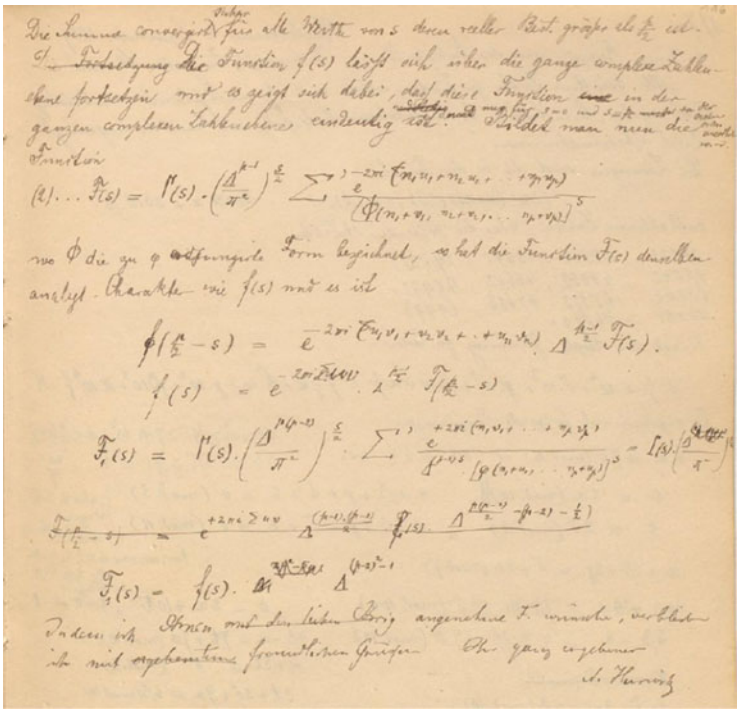


Fig. 16 Page 116 from the mathematical Diary no. 6, [51]

We conclude with another quotation from Pólya's text introducing the mathematical diaries of Adolf Hurwitz:

> Perhaps one will find in the diaries some more isolated pretty results and promising germ...[51]

Acknowledgements The photographs were taken from internet sources, and some of them are courtesy of the ETH library; most of the pictures stem from the webpages of the MacTutor History of Mathematics Archive at St. Andrews University, Scotland. We are grateful to these institutions for their support. Moreover, we would like to thank Klaus Volkert and Jürgen Wolfart for reading a former version of this article and for giving valuable hints. Last not least, we would like to express our gratitude to the organizers Jürgen Sander, Martin Kreh, and Jan-Hendrik de Wiljes of the conference *Elementare und analytische Zahlentheorie* at Hildesheim University in 2014 for the kind hospitality and their support to publish this volume in memory of Wolfgang Schwarz.

[51] "Wohl wird noch in den Tagbüchern manches hübsche Einzelresultat, mancher entwicklungsfähige Anregungskeim zu finden sein..."; [90, p. 7.].

References

1. G.L. Alexanderson, L.H. Lange, Obituary George Pólya. Bull. Lond. Math. Soc. **19**, 559–608 (1987)
2. T.M. Apostol, Remark on the Hurwitz zeta function. Proc. Am. Math. Soc. **2**, 690–693 (1951)
3. L. Bianchi, Letters of Luigi Bianchi to Adolf Hurwitz, Korrespondenz von Adolf Hurwitz, Cod Ms Math Arch 76, Niedersächsische Staats- und Universitätsbibliothek, Göttingen (1881)
4. L. Bianchi, *Opere*. Corrispondenza, vol. XI (Edizioni Cremonese, Roma, 1959)
5. Ch. Biehler, Sur une classe d'equation algébraiques dont toutes les racines sont réelles. Nouv. Ann. Math. **19**, 149–152 (1880)
6. K.-R. Biermann (ed.), *Briefwechsel zwischen Alexander von Humboldt und Peter Gustav Lejeune Dirichlet* (Akademie der Wissenschaften der DDR, Berlin, 1982)
7. U. Bottazini, J. Gray, *Hidden Harmony – Geometric Dantasies* (Springer, Berlin, 2013)
8. G. Burde, W. Schwarz, J. Wolfart, Max Dehn und das Mathematische Seminar der Universität Frankfurt im Fluss der Zeit. Algorismus **44**, 462–483 (2004)
9. E. Cahen, Sur la fonction $\zeta(s)$ de Riemann et sur des fonctions analogues. Ann. l'Éc. Norm. **XI**, 75–164 (1894)
10. M. Cantor, Nachruf an Oskar Schlömilch. Bibl. Math. **3**, 260–281 (1901)
11. T. Clausen, Beweis des Schlömilch Lehrsatzes. Arch. Math. Phys. **30**, 166–170 (1858)
12. G. Csordas, T.S. Norfolk, R.S. Varga, The Riemann hypothesis and the Turán inequalities. Trans. Am. Math. Soc. **296**, 521–541 (1986)
13. H. Davenport, *Multiplicative Number Theory* (Springer, New York, 1967)
14. H. Davenport, H. Heilbronn, On the zeros of certain Dirichlet series I, II. J. Lond. Math. Soc. **11**, 181–185, 307–312 (1936)
15. L. de Branges, *Hilbert Spaces of Entire Functions* (Prentice-Hall, London, 1968)
16. C.J. de la Vallée Poussin, Recherches analytique sur la théorie des nombres premiers, I-III. Ann. Soc. Sci. Bruxelles **20**, 183–256, 281–362, 363–397 (1896)
17. C.J. de la Vallée Poussin, Recherches analytique sur la théorie des nombres premiers, IV,V. Ann. Soc. Sci. Bruxelles **21**, 251–342, 343–368 (1897)
18. P.G.L. Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abh. Kgl. Preuß. Akad. Wiss. 45–81 (1837); Werke I, Reimer G, Berlin 313–342 (1889)
19. P.G.L. Dirichlet, Recherches sur diverses applications de l'analyse infinitésimale a la théorie des nombres. J. Reine Angew. Math. **19**, 324–369 (1839); **21**, 1–12 , 134–155 (1840), Werke I, Reimer G, Berlin 1889, 411–496
20. P.G.L. Dirichlet, *Vorlesungen über Zahlentheorie*, 3rd edn. (Vieweg, Kranzberg, 1879); with supplements by R. Dedekind
21. J. Elstrodt, The life and work of Gustav Lejeune Dirichlet (1805–1859), in *Analytic Number Theory: A Tribute to Gauss and Dirichlet*, ed. by W. Duke et al. Clay Mathematics Proceedings, vol. 7 (2007), pp. 1–37
22. P. Epstein, Zur Theorie allgemeiner zeta functionen. Math. Ann. **56**, 615–644 (1903)
23. L. Euler, Variae observationes circa series infinitas. Comment. Acad. Sci. Petropol **12**, 53–96 (1737/1744); Opera Omnia **I.14**, Teubner 407–462 (1924)
24. L. Euler, Demonstration de la somme de cette suite $1 + 1/4 + 1/9 + 1/16 + \ldots$. J. Lit. d'Allemagne Suisse Nord **2**, 115–127 (1743); Opera Omnia **I.14**, Teubner 1924, 138–155
25. L. Euler, Remarques sur un beau rapport entre les séries des puissances tant directes qui réciproques. Mém. l'Acad. Sci. Berlin **17** (1749/1768), 83–106; Opera Omnia **I.15**, Teubner 1924, 70–90
26. N.J. Fine, Note on the Hurwitz zeta-function. Proc. Am. Math. Soc. **2**, 361–364 (1951)
27. G. Frei, U. Stammbach, *Die Mathematiker an den Zürcher Hochschulen* (Birkhäuser, Basel, 1994)

28. F.G. Frobenius, Über Gruppencharaktere. Sitzber. Königlich Preuss. Akad. Wiss. Berlin, 985–1021 (1896)
29. R. Garunkštis, A. Laurinčikas, *The Lerch Zeta-function* (Kluwer, Dordrecht, 2002)
30. C.F. Gauss, *Werke, I* (Gesellschaft der Wissenschaften zu Göttingen, Göttingen, 1870)
31. St.S. Gelbart, St.D. Miller, Riemann's zeta function and beyond. Bull. Am. Math. Soc. **41**, 59–112 (2004)
32. J. Grommer, Ganze transzendente Funktionen mit lauter reellen Nullstellen. J. Reine Angew. Math. **144**, 114–165 (1914)
33. R. Haas, Goldbach, Hurwitz, and the infinitude of primes: weaving a proof across the centuries. Math. Intell. **36**, 54–60 (2013)
34. J. Hadamard, Essai sur l'étude des fonctions données par leur développement de Taylor. J. Math. **VIII**, 101–186 (1892)
35. J. Hadamard, Étude sur le propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann. J. Math. Pures Appl. **9**, 171–215 (1893)
36. J. Hadamard, Sur les zéros de la fonction $\zeta(s)$ de Riemann. C. R. **122**, 1470–1473 (1896)
37. J. Hadamard, Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. Bull. Soc. Math. France **24**, 199–220 (1896)
38. H. Hamburger, Über einige Beziehungen, die mit der Funktionalgleichung der Riemannschen ζ-Funktion äquivalent sind. Math. Ann. **85**, 129–140 (1922)
39. H. Hankel, Die Euler'schen Integrale bei unbeschränkter Variabilität der Arguments. Habilitations-Diss. (Leipzig, 1863)
40. G.H. Hardy, Sur les zéros de la fonction $\zeta(s)$ de Riemann. C. R. Acad. Sci. Paris **158**, 1012–1014 (1914)
41. H. Hasse, Ein Summierungsverfahren für die Riemannsche ζ-Reihe. Math. Z. **32**, 458–464 (1930)
42. St. Hawking, Zeta function regularization of path integrals in curved spacetime. Commun. Math. Phys. **55**, 133–148 (1977)
43. E. Hecke, Über die Zetafunktionen beliebiger algebraischer Zahlkörper. Nachr. Ges. Wiss. Göttingen, 77–89 (1917)
44. E. Hecke, Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung. Math. Ann. **112**, 664–699 (1936)
45. D. Hejhal, On a result by G. Pólya concnerning the Riemann ξ-function. J. Analyse Math. **55**, 59–95 (1990)
46. A. Hurwitz, Einige Eigenschaften der Dirichletschen Funktionen $F(s) = \sum \left(\frac{D}{n}\right) \frac{1}{n^s}$, die bei der Bestimmung der Klassenzahlen binärer quadratischer Formen auftreten. Z. Math. Phys. **27**, 86–101 (1882)
47. A. Hurwitz, Ueber die Nullstellen der Bessel'schen Function. Math. Ann. **33**, 246–266 (1889)
48. A. Hurwitz, Review to [9]. Jahresberichte JFM 25.0702.01
49. A. Hurwitz, Sur les points critiques des fonctions inverses dse fonctions entières. C. R. **158**, 1007–1008 (1914)
50. A. Hurwitz, *Lectures on Number Theory* (Springer, New York, 1985); translated from unpublished German course notes by N. Kritikos
51. A. Hurwitz, *Die Mathematischen Tagebücher und der übrige handschriftliche Nachlass von Adolf Hurwitz*. Handschriften und Autographen der ETH Zürich (1919). http://www.e-manuscripta.ch/
52. H. Iwaniec, *Lectures on the Riemann Zeta Function* (AMS, Providence, 2014)
53. J.L.W.V. Jensen, Undersøgelser over Ligningernes Theori. Beretning om den anden skandinaviske Matematikerkongres i Kjøbenhavn 51–65 (1911)
54. A. Jonquière, Note sur la série $\sum_{n=1}^{\infty} \frac{x^n}{n^s}$. Bull. Soc. Math. France **17**, 142–152 (1889)
55. H. Kinkelin, Allgemeine Theorie der harmonischen Reihen, mit Anwendungen auf die Zahlentheorie. Programm der Gewerbeschule Basel 1–32 (1861/1862)
56. H. Koch, Oskar Xaver Schlömilch – ein Förderer des mathematischen Unterrichts für Techniker und Ingenieure. NTM, Schriftenr. Gesch. Naturwiss. Tech. Med. **27**, 1–10 (1990)

57. L. Kronecker, Notiz über Potenzreihen. Monatsber. Preuss. Akad. Wiss. Berlin 53–58 (1878); Werke **V**, Teubner, Leipzig 1930, 197–201
58. E. Landau, Euler und die Funktionalgleichung der Riemannschen Zetafunktion. Bibl. Mat. **7**, 69–79 (1906)
59. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*. Zwei Bänden (Teubner, Leipzig, 1909)
60. E. Landau, *Vorlesungen über Zahlentheorie* (Zweiter Band, Hirzel/Leipzig, 1927)
61. S. Lang, *Introduction to Modular Forms* (Springer, Berlin, 1976)
62. S. Lang, *Complex Analysis*, 4th edn. (Springer, Berlin, 1999)
63. D. Laugwitz, *Bernhard Riemann 1826–1866* (Birkhäuser, Boston, 2008). English translation
64. A.M. Legendre, *Essai sur la théorie des nombres*, 2nd edn. (Courcier, Paris, 1808)
65. M. Lerch, Sur la fonction $\mathcal{K}(w,x,s) = \sum_{k=0}^{\infty} \frac{\exp(2k\pi ix)}{(w+k)^s}$. Acta Math. **11**, 19–24 (1887/1888)
66. M. Lerch, Základove theorie Malmstènovych řad. Rozpravy Českè Akad. 2.Kl. **1**, 1–70 (1892)
67. E. Lindelöf, Robert Hjalmar Mellin. Acta Math. **61**, i-vii (1933)
68. R. Lipschitz, Untersuchung einer aus vier Elementen gebildeten Reihe. J. Reine Angew. Math. **54**, 313–328 (1857)
69. R. Lipschitz, Untersuchungen der Eigenschaften einer Gattung von unendlichen Reihen. J. Reine Angew. Math. **105**, 127–156 (1889)
70. C.J. Malmstèn, De integralibus quibusdam definitis, seriebusque infinitis. J. Reine Angew. Math. **38**, 1–39 (1849); An English translation due to A. Aycock is available as arXiv:1309.3824v1
71. Hj. Mellin, Über eine verallgemeinerung der riemannschen function $\zeta(s)$. Acta Soc. Sci. Fenn. **24**(10), 50 p. (1899)
72. Hj. Mellin, Die Dirichlet'schen Reihen, die zahlentheoretischen Funktionen und die unendlichen Produkte von endlichem Geschlecht. Acta Math. **28**, 37–64 (1904)
73. F. Mertens, Beweis, dass jede linerae Function mit ganzen complexen teilerfremden Coefficienten unendlich viele complexe Primzahlen darstellt. Wien Ber. **108**, 517–556 (1899)
74. H. Minkowski, Peter Gustav Lejeune Dirichlet und seine Bedeutung für die heutige mathematik. Jahresber. Dtsch. Math. Ver. **14**, 149–163 (1905)
75. H. Minkowski, *Briefe an David Hilbert*, ed. by L. Rüdenberg, H. Zassenhaus (Springer, Berlin, 1973)
76. M.R. Murty, N. Thain, Prime numbers in certain arithmetic progressions. Funct. Approx. Comment. Math. **35**, 249–259 (2006)
77. W. Narkiewicz, *The Development of Prime Number Theory* (Springer, New York, 2000)
78. N.M.R. Oswald, J. Steuding, Complex continued fractions: early work of the brothers Adolf and Julius Hurwitz. Arch. Hist. Exact Sci. **68**, 499–528 (2014)
79. N.M.R. Oswald, J. Steuding, About the cover: zeta-functions associated with quadratic forms in Adolf Hurwitz's estate. Bull. Am. Math. Soc. New Ser. **53**, 477–481 (2016)
80. O. Perron, Zur Theorie der Dirichletschen Reihen. J. Reine Angew. Math. **134**, 95–143 (1908)
81. S. Poisson, *Theorie Mathématiques de la Chaleur* (Bachelier, Paris, 1835)
82. G. Pólya, Über Annäherung durch Polynome mit lauter reellen Wurzeln. Rend. Circ. Mat. Palermo **36**, 279–295 (1913)
83. G. Pólya, Sur une question concernant les fonctions entières. C. R. Acad. Sci. Paris **158**, 330–333 (1914)
84. G. Pólya, Ueber die Nullstellen gewisser ganzer funktionen. Math. Z. **2**, 352–383 (1918)
85. G. Pólya, Bemerkung über die Integraldarstellung der Riemannschen ξ-Funktion. Acta Math. **48**, 305–317 (1926)
86. G. Pólya, On the zeros of certain trigonometric integrals. J. Lond. Math. Soc. **1**, 98–99 (1926)
87. G. Pólya, Über die algebraisch-funktionentheoretischen Untersuchungen von J. L. W. Jensen. Meddelelser Kobenhavn **7**, 3–33 (1927)
88. G. Pólya, Über trigonometrische Integrale mit nur reellen Nullstellen. J. Reine Angew. Math. **158**, 6–18 (1927)

89. G. Pólya, Letter exchange between Pólya and Odlyzko (1982). Available at www.dtc.umn.edu/~odlyzko/polya/
90. G. Pólya, Über den handschriftlichen Nachlass des Mathematikers Adolf Hurwitz. Handschriften und Autographen der ETH-Bibliothek (1921)
91. G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis I, II* (Springer, Berlin, 1925)
92. Št. Porubský, Matyáš Lerch (1860–1922). Šiauliai Math. Semin. **8**(16), 197–222 (2013)
93. B. Riemann, Über die Anzahl der Primzahlen unterhalb einer gegebenen Grösse. Monatsber. Preuss. Akad. Wiss. Berlin 671–680 (1859)
94. D.E. Rowe, Felix Klein, Adolf Hurwitz, and the "Jewish Question" in German academia. Math. Intell. **29**, 18–30 (2007)
95. D.E. Rowe, R. Schulmann, General relativity in the context of Weimar culture. Max-Planck-Inst. Wiss. 456 (2014, preprint)
96. I. Samuel-Hurwitz, Erinnerungen an die Familie Hurwitz, mit Biographie ihres Gatten Adolph Hurwitz, Prof. f. höhere Mathematik an der ETH, HS 583a: 2, Archive ETH Zurich University Archives (1984)
97. G. Schaertlin, Hermann Kinkelin. Mitt. Schweizerischer versicherungsmathematiker **28**, 1–17 (1933)
98. W. Scharlau, The mathematical correspondence of Rudolf Lipschitz. Hist. Math. **13**, 165–167 (1986)
99. H. Scheibner, Ueber die Anzahl der Primzahlen unter einer beliebigen Grenze. Z. Math. **5**, 233–252 (1860)
100. O. Schlömilch, Uebungsaufgaben für Schüler ueber den Lehrsatz von dem Herrn Prof. Dr. Schlömilch. Arch. Math. Phys. **12**, 415 (1849)
101. O. Schlömilch, Über eine Eigenschaft gewisser Reihen. Z. Math. Phys. **3**, 130–132 (1858)
102. O. Schlömilch, Ueber die Summen von Potenzen der reciproken natürlichen Zahlen. Z. Math. Phys. **23**, 135–137 (1878)
103. W. Schnee, Die Funktionsgleichung der Zetafunktion und der Dirichletschen Reihen mit periodischen Koeffizienten. Math. Z. **31**, 378–390 (1929)
104. W. Schwarz, Some remarks on the history of the prime number theorem from 1896 to 1960, in *Development of Mathematics 1900–1950*, ed. by J.-P. Pier (Birkhäuser, Basel, 1994), pp. 565–616
105. A. Selberg, Old and new conjectures and results about a class of Dirichlet series, in *Proceedings of the Amalfi Conference on Analytic Number Theory, Maiori 1989*, ed. by E. Bombieri et al. (Università di Salerno, 1992), pp. 367–385
106. C.L. Siegel, Über Riemanns Nachlaß zur analytischen Zahlentheorie. Quell. Stud. Gesch. Mat. Astr. Phys. **2**, 45–80 (1932)
107. C.L. Siegel, The average measure of quadratic forms with given determinant and signature. Ann. Math. **45**, 667–685 (1944)
108. C.L. Siegel, Zur geschichte des frankfurter mathematischen seminars, in *Gesammelte Abhandlungen*, vol. III (Springer, Berlin, 1966)
109. J. Tate, Fourier analysis in number fields, and Hecke's zeta-functions, in *Algebraic Number Theory: Proceedings of on Instructional Conference on Brighton 1965* (Thompson, Washingthon, 1967), pp. 305–347
110. E.C. Titchmarsh, On Epstein's zeta-function. Proc. Lond. Math. Soc. **36**, 485–500 (1934)
111. H. von Mangoldt, Zu Riemann's Abhandlung "Ueber die Anzahl der Primzahlen unter einer gegebenen Größe". J. Reine Angew. Math. **114**, 255–305 (1895)
112. A. Weil, Prehistory of the zeta-function, in *Number Theory, Trace Formulas and Discrete Groups (Oslo, 1987)*, ed. by E.A. Aubert et al. (Academic, Boston, 1989), pp. 1–9
113. A. Weil, On Eisenstein's copy of the disquisitiones, in *Algebraic Number Theory – In Honor of K. Iwasawa; Proceeding of a Workshop Iwasawa Theory Spec. Values L-Functions*, Berkeley, 1987. Adv. Stud. Pure Math., vol. 17 (1989), pp. 463–469

Selberg Sums: A New Perspective

Samuel J. Patterson

To the memory of Wolfgang Schwarz

Abstract Selberg sums are the analogues over finite fields of certain integrals studied by Selberg in 1940s. The original versions of these sums were introduced by R.J. Evans in 1981, and following an elegant idea of G.W. Anderson in 1991 they were evaluated by Anderson, Evans and P.B. van Wamelen. In 2007 the author noted that these sums and certain generalizations of them appear in the study of the distribution of Gauss sums over a rational function field over a finite field. The distribution of Gauss sums is closely related to the distribution of the values of the discriminant of polynomials of a fixed degree. Here we shall take this up further. The main goal here is to establish the basic properties of Selberg sums and to formulate the problems which arise from this point of view.

Keywords Anderson–Evans–v.Wamelen theorem • Eisenstein series • Metaplectic groups • Rational function fields • Selberg sums

2010 Mathematics subject classification: Primary 11T24; Secondary 11T55, 11F99

1 Introduction

The usual class of character sums known as Selberg sums was introduced in 1981 by Evans [5]. They were the analogues over finite fields of a class, or rather several related classes, of integrals introduced by A. Selberg in 1944, [12, p. 204 ff.]. In fact he had already used an integral of this type in 1941 in [12, p. 74 ff.] but was uncertain as to whether the integral was already known and waited before publishing details.

S.J. Patterson (✉)
Mathematisches Institut, Bunsenstr. 3–5, 37073 Göttingen, Germany
e-mail: Samuel.James.Patterson@mathematik.uni-goettingen.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_21

Characteristic of these integrals is that they are taken over a space of monic polynomials of a fixed degree and that one factor in the integrand is a power of the discriminant. Selberg regarded the integrals he studied as an extension of Euler's beta-function and, indeed, his evaluation gives the integrals as a quotient of products of gamma functions. The primary example is the integral

$$\int_0^1 \cdots \int_0^1 (x_1 \cdots x_i)^{\alpha-1}((1-x_1)\cdots(1-x_n))^{\beta-1} |\prod_{i<j}(x_i - x_j)|^{2\gamma} \mathrm{d}x_1 \cdots \mathrm{d}x_i$$

in the region $\mathrm{Re}(\alpha) > 0$, $\mathrm{Re}(\beta) > 0$, $\mathrm{Re}(\gamma) > -\mathrm{Min}(\frac{1}{i}, \frac{\mathrm{Re}(\alpha)}{i-1}, \frac{\mathrm{Re}(\beta)}{i-1})$. Selberg's evaluation shows that the integral is equal to

$$\prod_{j=1}^{i} \frac{\Gamma(1+j\gamma)\Gamma(\alpha+(j-1)\gamma)\Gamma(\beta+(j-1)\gamma)}{\Gamma(1+\gamma)\Gamma(\alpha+\beta+(i+j-2)\gamma)}.$$

For our purposes a transformation is helpful. This integral can be regarded as over all monic polynomials of degree i with all their roots in $[0, 1]$. We let $\sigma_1, \ldots, \sigma_i$ be the standard symmetric functions in $x_1, \ldots, x_i$. Then one has

$$\mathrm{d}\sigma_1 \wedge \mathrm{d}\sigma_2 \wedge \cdots \wedge \mathrm{d}\sigma_i = \prod_{j<j'}(x_j - x_{j'})\ \mathrm{d}x_1 \wedge \mathrm{d}x_2 \wedge \cdots \wedge \mathrm{d}x_i.$$

It follows that we can write Selberg's integral as

$$\int |f(0)|^{\alpha} |f(1)|^{\beta} |D(f)|^{\gamma-\frac{1}{2}} \mathrm{d}f,$$

where the integral is over the set of polynomials described above and $\mathrm{d}f$ is the standard Lebesgue measure on the affine space of the f.

We can now describe Evans' analogue. Let q be a power of the odd prime number p. Let χ_1, χ_2, and χ_3 be multiplicative characters on $\mathbf{F}_q^{\times}$ and let ω be the unique quadratic character. Then Evans introduces

$$\sum \chi_1(f(0))\chi_2(f(1))(\omega\chi_3)(D(f))$$

where $D(f)$ denotes the discriminant of the polynomial f and the sum is taken over all monic polynomials of a fixed degree i. It turns out that introducing the factor ω makes the development much smoother and it can be regarded as the analogue of the term $-\frac{1}{2}$ in the exponent of $D(f)$ in the alternative version of Selberg's integral.

In 1990 Anderson [1] found an ingenious and remarkably simple method for evaluating some of these sums. Following this first Evans [6] and then van Wamelen [15] extended Anderson's method to cover all cases. Details of the results are given in Sect. 3.

Since Selberg's integral can be considered as an extension of the beta-integral we can regard Evans' sum as an extension of their analogues over finite fields, namely Jacobi sums. One immediate generalization of the beta-integral is the standard integral representation of the hypergeometric function and their generalizations. In [10] it was pointed out that the finite field analogues of these functions intervene in the theory of metaplectic forms, and especially of Eisenstein series, over rational function fields over finite fields. In this chapter we shall follow this line of thought and apply the appellation "Selberg sum" to this more general class of sum. To the best of my knowledge the corresponding Archimedean functions have not been investigated.

The theory of metaplectic forms leads us to the evaluation to some more general Selberg sums. This is an aspect which we shall not go into here; some indications are given in [11]. He we shall take up a theme of that paper, namely a transformation formula. This will be given in Sect. 4. It is quite elementary but among other things it shows that the results of Anderson, Evans, and v.Wamelen can be used to evaluate further interesting classes of Selberg sums.

It is worth noting that it is relatively easy to compute specific examples of Selberg sums and so one can investigate them experimentally. We shall explain why this is so later. This means that one can investigate the sums experimentally and, for example, examine their sizes in various metrics. This is a topic which we shall postpone to a later paper.

My thanks are due to Ben Brubaker, Paul Gunnells, and Zeev Rudnick for helpful conversations about the topics discussed in this paper.

2 Notations

Let, as before, q be a power of the odd prime q. For $f, g \in \mathbf{F}_q[x]$ let $R(f,g)$ be the resultant of $R(f,g)$ We recall that $R(f,g)$ is a universal polynomial (Sylvester's determinant) in the coefficients of f and g. The function $g \mapsto R(f,g)$ depends only on $g \pmod f$. Also $R(f,g)$ is bimultiplicative and satisfies the reciprocity law

$$R(g,f) = (-1)^{\deg(f)\deg(g)} R(f,g).$$

Finally $R(x-a,f) = f(a)$. These properties determine R completely and can be cast into the form of an efficient algorithm based on the model of continued fractions for its evaluation.

For $f \in \mathbf{F}_q[x]$ let $D(f)$ be the discriminant of f. If f is monic one has $D(f) = \eta(\deg(f))R(f,f')$ where $\eta(i) = 1$ for $i \equiv 0, 1 \pmod 4$ and $\eta(i) = -1$ for $i \equiv 2, 3 \pmod 4$.[1]

[1]Note that this factor is missing from the formula (5) on [14, p. 87], an oversight which unfortunately led to author to similar inaccuracies in [10].

We let μ be the Möbius function on $\mathbf{F}_q[x]$. Then Pellet's formula (see [2, (1.5)], [4, Lemma 4.1], or [13]) asserts that

$$\mu(f) = (-1)^{\deg(f)}\omega(D(f))$$

where, as above, ω is the unique quadratic character on $\mathbf{F}_q^\times$.

Let X_q be the group of characters on $\mathbf{F}_q^\times$ which we consider as taking values in $\mathbf{Q}(1^{\frac{1}{q-1}})$. For $\chi \in X_q$ let $\mathrm{ord}(\chi)$ denote the order of χ. Let e_o be a nontrivial additive character on $\mathbf{F}_q$; for our purposes it is convenient to regard it as taking values in $\mathbf{Q}(1^{\frac{1}{p}})$. The choice of e_o will not play any significant role in our discussion. For $\chi \in X_q$ we define the Gauss sum over $\mathbf{F}_q$ to be

$$\tau(\chi) = \sum_{a \in \mathbf{F}_q^\times} \chi(a) e_o(a).$$

For $\chi_1, \chi_2 \in X_q$ let

$$J(\chi_1, \chi_2) = \sum_{\substack{a \in \mathbf{F}_q \\ a \neq 0,1}} \chi_1(a)\chi_2(1-a)$$

be the Jacobi sum. Then if $\chi_1\chi_2 \neq 1$

$$\tau(\chi_1)\tau(\chi_2) = J(\chi_1, \chi_2)\tau(\chi_1\chi_2)$$

whereas if $\chi_1\chi_2 = 1$, but $\chi_1, \chi_2 \neq 1$ then

$$\tau(\chi_1)\tau(\chi_2) = \chi_1(-1)q$$

and

$$J(\chi_1, \chi_2) = -\chi_1(-1).$$

Additionally one has $J(\chi, 1) = -1$ if $\chi \neq 1$ and $J(1, 1) = q - 2$. Also $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$, $J(\chi_1, \chi_2) = \chi_2(-1)J((\chi_1\chi_2)^{-1}, \chi_2)$ and $J(\chi_1, \chi_2) = \chi_1(-1)J(\chi_1, (\chi_1\chi_2)^{-1})$. There are some further relations and properties of these sums which have been studied in great detail.

Let now $k = \mathbf{F}_q(x)$ and $R = \mathbf{F}_q[x]$. We define

$$e : k \to \mathbf{Q}(1^{\frac{1}{p}})$$

by

$$\begin{aligned} e(f) &= e_o\Big(\textstyle\sum_{v \neq \infty} \mathrm{Res}_v(f\mathrm{d}x)\Big) \\ &= e_o(-\mathrm{Res}_\infty(f\mathrm{d}x)). \end{aligned}$$

Here, in the sum, v runs through the finite places of k.

We define for $\chi \in X_q$ and $g \in R - \{0\}$ the Dirichlet character of modulus g

$$f \mapsto \chi(f/g) = \chi(R(g,f)).$$

We define the global Gauss sum associated with k to be

$$g(r,\chi,c) = \sum_{d \pmod c} \chi(d/c)e(rd/c)$$

for $r \in R - \{0\}$. This can, by means of the Davenport–Hasse theorem, be evaluated in terms of Gauss sums over $\mathbf{F}_q$. If r is coprime to c one obtains

$$g(r,\chi,c) = \mu(c)\chi(r/c)^{-1}\chi(c'/c)(-\tau(\chi))^{\deg(c)}.$$

Here c' denotes the derivative of c. This shows that the function $\chi(c'/c)$ is as subtle a function of c as $g(r,\chi,c)$. Recall that it is equal to $\chi(\eta(\deg(c)))\chi(D(c))$ for c monic. We therefore have for c coprime to r

$$g(r,\chi,c) = \mu(c)\chi(\eta(\deg(c)))\chi(r/c)^{-1}(-\tau(\chi))^{\deg(c)}\chi(D(c)).$$

In the special case $\chi = \omega$, $r = 1$ we obtain

$$g(r,\omega,c) = \mu(c)^2\omega(\eta(\deg(c)))\tau(\omega)^{\deg(c)}.$$

As $\tau(\omega)$ is $\sqrt{q}$ times a fourth root of 1 this gives us the Gauss evaluation of the quadratic Gauss sum in this context. One could also use this argument to prove Pellet's formula using that evaluation, as given, for example, in [16, XIII, Sect. 11, Proof of Theorem 13].

We can now define the Selberg sums which we are going to investigate here. Apart from a factor ± 1 it specializes to the one used in the papers of Anderson, Evans, and v. Wamelen when we take r to be of the form $x^{e_0}(x-1)^{e_1}$. For χ_1, χ_2 it is

$$\sum_c \chi_1(r/c)\omega(D(c))\chi_2(D(c))$$

where c is summed over all monic polynomials of a fixed degree i. For our purposes it is convenient to modify the expression by using Pellet's formula. It becomes

$$(-1)^i \sum_c \mu(c)\chi_1(r/c)\chi_2(D(c)),$$

or, with the reciprocity law,

$$(-1)^i\chi(-1)^{i\deg(r)i} \sum_c \mu(c)\chi_1(c/r)\chi_2(D(c)).$$

Both of the sums here could be considered as to be entitled to be the more fundamental one. We choose

$$Se(r, \chi_1, \chi_2, i) = \sum_{\substack{c \text{ monic} \\ \deg(c)=i}} \mu(c)\chi_1(r/c)\chi_2(D(c)).$$

We take $\chi_1(r/c)$ to be zero if r and c are not coprime. By means of the Davenport–Hasse theorem we have then

$$Se(r, \chi_1, \chi_2, i) = (-1)^i \tau(\chi_2)^{-i} \chi_2(\eta(i)) \sum_{\substack{c \text{ monic} \\ \deg(c)=i}} \chi_1(r/c) g(1, \chi_2, c).$$

If now there exists an exponent e so that

$$\chi_1 \chi_2^e = 1$$

then

$$Se(r, \chi_1, \chi_2, i) = (-1)^i \tau(\chi_2)^{-i} \chi_2(\eta(i)) \sum_{\substack{c \text{ monic} \\ \deg(c)=i}} g(r^e, \chi_2, c)$$

where we restrict the sum to c coprime to r. In this case one can use the theory of metaplectic forms to investigate these sums, see [10, 11]. At the other extreme $\chi_2 = 1$ and $Se(r, \chi_1, 1, i)$ is then the coefficient of q^{-is} in the L-series $L(s, \chi_1(r/\cdot))$ (over R). It follows from this that if $\chi_1(r/\cdot)$ is non-principal then $Se(r, \chi_1, 1, i) = 0$ for $i \geq \deg(r_0)$ where r_0 is the conductor of $\chi_1(r/\cdot)$—[1, p. 471].

We should note that for r of the form θr_o^a with $\theta \in \mathbf{F}_q^\times$, $a \in \mathbf{N}$ one has

$$Se(r, \chi_1, \chi_2, i) = \chi_1(\theta)^i Se(r_o, \chi_1^a, \chi_2, i).$$

In particular we can reduce the calculation of $Se(r, \chi_1, \chi_2, i)$ to the case where r is monic.

3 The Anderson–Evans–v.Wamelen Evaluation of Selberg Sums

In this section we shall summarize the results of Anderson, Evans, and v.Wamelen in a notation suitable for the purposes in hand. We shall take $r(x) = x^{e_0}(x-1)^{e_1}$. The group X_q is cyclic and the notation of these three authors is based on the choice of a generator denoted by τ. The parameters a, b, and c are related to the parameters here by $\tau^a = \chi_1^{e_0}$, $\tau^b = \chi_1^{e_1}$, and $\tau^c = \chi_2$. It is convenient to distinguish two cases. If

$\tau^a = \chi_1^{e_0}$ and $\tau^b = \chi_1^{e_1}$ lie in the subgroup generated by $\tau^c = \chi_2$ then we can define two integers f_0 and f_1 by $\chi_1^{e_0}\chi_2^{f_0} = 1$ and $\chi_1^{e_1}\chi_2^{f_1} = 1$. It turns out that it is this case, the one investigated by van Wamelen in [15], is precisely the one covered by the theory of metaplectic forms as formulated in [11]. We shall therefore refer to this as the *metaplectic* case. The alternative, when either $\chi_1^{e_0}$ or $\chi_1^{e_1}$ is not in the subgroup of X_q generated by χ_2 we call *non-metaplectic*. This was the one investigated by Evans in [6]. This nomenclature is by no means satisfactory, nor even accurate, but it has developed from my private usage and I have not found anything better to propose. The distinction does seem to be a useful one as we shall see below.

In the discussion below we shall write i instead of n as used by Anderson, Evans, and v.Wamelen. This corresponds to the usage in Sect. 2. We shall also use n, the order of χ_2, where they used d. For $m \in \mathbf{N}$ and $j \in \mathbf{Z}$ we write $(j)_m$ for the least non-negative residue of j modulo m.

In the theory of Selberg sums a particularly important role is played by a product denoted by previous authors by $P_n(a, b, c)$ and which we shall replace by

$$P_i(e_0, e_1, \chi_1, \chi_2) = \prod_{0 \le j < i} \frac{\tau(\chi_1^{e_0}\chi_2^j)\tau(\chi_1^{e_1}\chi_2^j)\tau(\chi_2^{j+1})\overline{\tau(\chi_1^{e_0+e_1}\chi_2^{i-1+j})}}{q\tau(\chi_2)}.$$

This product corresponds to Selberg's product of gamma functions. It is clear that for a certain A one has

$$P_{i+\ell n}(e_0, e_1, \chi_1, \chi_2) = A^\ell P_i(e_0, e_1, \chi_1, \chi_2).$$

One can express A in a simple form, [6, Lemma 3.1],

$$\begin{aligned} A &= q^{n-2}\chi_2(\eta(n))/\tau(\chi_2)^n && \text{in the metaplectic case} \\ &= -J(\chi_1^{e_0 n}, \chi_1^{e_1 n})q^{n-1}\chi_2(\eta(n))/\tau(\chi_2)^n && \text{in the non-metaplectic case.} \end{aligned}$$

Note that in the latter case at least one of $\chi_1^{e_0 n}$ and $\chi_1^{e_1 n}$ is nontrivial. Our notations are the reason that this looks a little different from the formulation in [6].

It is worth-while noting that in [15, Lemma 2] van Wamelen proves the additional evaluation that $P_{f_0+f_1+1}(e_0, e_1, \chi_1, \chi_2)$ is equal to

$$-q^{(f_0+f_1)_n - 1}\chi_1(-1)^{f_0+f_1+1}\chi_2(\eta(f_0+f_1+1))\frac{\tau(\chi_2^{f_0+f_1+1})}{\tau(\chi_2)^{f_0+f_1+1}}.$$

These evaluations are consequences of the Davenport–Hasse analogue of the Gauss–Legendre multiplication formula for the gamma function.

For $y \in \mathbf{N}$ let

$$T(y, q) = -y + \sum_{k=0}^{y}(2k+1)(-q)^{y-k}$$

and

$$S(y,q) = 1 - (1-q)y.$$

From now on we shall assume the $n > 1$ as Anderson's argument has to be modified in the exceptional case $n = 1$. For more details see Sect. 5. The main result of the three authors is that in the non-metaplectic case

$$Se(x^{e_0}(x-1)^{e_1}, \chi_1, \chi_2, i)$$

is equal to

$$\chi_1(-1)^{e_1 i}(-1)^i P_i(e_0, e_1, \chi_1, \chi_2)$$

and in the metaplectic case it is equal to

$$\chi_1(-1)^{e_1 i}(-1)^i q^{\left[\frac{i}{n}\right]} P_i(e_0, e_1, \chi_1, \chi_2)$$

times

$$\begin{array}{ll} T(2\left[\frac{i}{n}\right], q) & \text{if } (i)_n \leq \text{Min}(f_0,f_1) \leq \text{Max}(f_0,f_1) < (f_o + f_1 - i + 1)_n \\ T(2\left[\frac{i}{n}\right] + 1, q) & \text{if } (f_o + f_1 - i + 1)_n \leq \text{Min}(f_0,f_1) \leq \text{Max}(f_0,f_1) < (i)_n \\ S(\left[\frac{i}{n}\right] + 1, q) & \text{otherwise.} \end{array}$$

We note here, following [15, Sect. 4], the following summations,

$$\sum_{m \geq 0} T(2m, q) X^m = \frac{U_e(q, X)}{(1-X)^2(1-q^2X)}$$

where

$$U_e(q, X) = 2X^2q^2 - qX^2 - 3qX + X + 1,$$

$$\sum_{m \geq 0} T(2m+1, q) X^m = \frac{U_o(q, X)}{(1-X)^2(1-q^2X)}$$

where

$$U_o(q, X) = X^2q^2 + q^2X - 3qX - q + 2,$$

and

$$\sum_{m \geq 0} S(m, q) X^m = \frac{1 + (q-2)X}{(1-X)^2}.$$

We note also that $U_e(q,q^{-2}) = (1-q^{-1})^3$, $U_e(q,1) = 2(q-1)^2$, $U_o(q,q^{-2}) = -q(1-q^{-1})^3$ and $U_o(q,1) = 2(q-1)^2$. These results mean that in the non-metaplectic case and in any complex embedding we have

$$\sum_{\substack{i\geq 0\\ i\equiv i_0}} S(x^{e_0}(x-1)^{e_1},\chi_1,\chi_2,i)X^{(i-i_0)/n}$$

is equal to

$$\chi_1(-1)^{e_1 i_0}(-1)^{i_0}P_{i_0}(e_0,e_1,\chi_1,\chi_2)/(1-\chi_1(-1)^{e_1 n}(-1)^n AX)$$

where we assume that $0 \leq i_0 < n$ and A is as above. Note that $|A|$ takes on, if $n \neq 1$, one of the three values $q^{\frac{n}{2}-1}$, $q^{\frac{n}{2}-\frac{1}{2}}$ or $q^{\frac{n}{2}}$ in any complex embedding. If $n = 1$ then $|A|$ takes on one of the three values 1, $q^{\frac{1}{2}}$ or q in any complex embedding.

In the metaplectic case we find that, according to the three cases above, the series is equal to

$$\chi_1(-1)^{e_1 i_0}(-1)^{i_0}\frac{P_{i_0}(e_0,e_1,\chi_1,\chi_2)U_e(q,\chi_1(-1)^{e_1 n}(-1)^n AX)}{(1-\chi_1(-1)^{e_1 n}(-1)^n qAX)^2(1-\chi_1(-1)^{e_1 n}(-1)^n q^3 AX)},$$

$$\chi_1(-1)^{e_1 i_0}(-1)^{i_0}\frac{P_{i_0}(e_0,e_1,\chi_1,\chi_2)U_0(q,\chi_1(-1)^{e_1 n}(-1)^n)AX}{(1-\chi_1(-1)^{e_1 n}(-1)^n qAX)^2(1-\chi_1(-1)^{e_1 n}(-1)^n q^3 AX)},$$

or

$$\chi_1(-1)^{e_1 i_0}(-1)^{i_0}\frac{P_{i_0}(e_0,e_1,\chi_1,\chi_2)(1+(q-2)\chi_1(-1)^{e_1 n}(-1)^n qAX)^2}{(1-\chi_1(-1)^{e_1 n}(-1)^n qAX)^2}$$

respectively. Note that the nature of the singularities reflect the type of the Selberg sum. As we have assumed that $n > 1$ we have in the metaplectic case $|A| = q^{\frac{n}{2}-2}$.

4 The Transformation Formula

We shall now turn to a property of Selberg sums analogous to Theorem 1 of [11]. We need some preparations in order to be able to formulate the result. Let n be the order of χ_2 and let n' be the order of χ_1. Let χ_0 be such that χ_1 and χ_2^2 are in the group generated by χ_0. Let $a \geq 0$ and $b \geq 0$ be such that

$$\chi_1 = \chi_0^a,\ \chi_2^2 = \chi_0^b.$$

Let π monic and a prime in $R = \mathbf{F}_q[x]$. If $\pi | r$ then

$$Se(\pi^{n'}r,\chi_1,\chi_2,i) = Se(r,\chi_1,\chi_2,i).$$

If $\pi \not| r$ this is no longer true. We have that

$$Se(r, \chi_1, \chi_2, i) - Se(\pi^{n'} r, \chi_1, \chi_2, i)$$

is equal to

$$\sum_{\deg(c_1\pi)=i} \mu(c_1\pi)\chi_1(r/c_1\pi)\chi_2(D(c_1\pi)).$$

Since $D(c_1\pi) = D(c_1)D(\pi)R(c_1, \pi)^2$ this becomes

$$-\chi_1(r/\pi)\chi_2(D(\pi)) \sum_{\deg(c_1)=i-\deg(\pi)} \mu(c_1)\chi_1(r/c_1\pi)\chi_2(\pi/c_2)^2\chi_2(D(c_1))$$

or

$$-\chi_1(r/\pi)\chi_2(D(\pi)Se(r^a\pi^b, \chi_0, \chi_2, i - \deg(\pi)).$$

We regard this as a stability property of Selberg sums.

Theorem 1 *Let $\alpha, \beta, \gamma, \delta \in \mathbf{F}_q$ be such that $\Delta = \alpha\delta - -\beta\gamma \neq 0$. Then for suitable integers M, M' we have that*

$$\chi_2(\Delta)^{1-i} Se\left(r\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right)^a \left(\frac{1}{(\gamma x+\delta)^2}\right)^{b(i-1)+M}, \chi_0, \chi_2, i\right)$$

is equal to

$$Se(r(x)(-\gamma x+\alpha)^{M'}, \chi_1, \chi_2, i)$$

If $\gamma = 0$ we can take $M, M' = 0$. If $\gamma \neq 0$ then M is to such that $\chi_0^M = 1$ and $M + b(i-1) > a \cdot \deg(r)$, and M' is such that $M' > 0$ and $\chi_1^{M'} = 1$.

Proof The proof is carried out by verifying the identity for $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, of the form $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ and equal to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and then combining these in the usual manner.

The first two cases are straightforward; we need to only replace c in the sum defining the Selberg sum by $c(x + \lambda)$ and $c(\theta x)\theta^{-i}$ where $\theta = \alpha/\delta$ respectively.

In the case $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ we assume that $r(0) = 0$; this is the reason for the introduction of the parameter M'. This being so c is not divisible by x and so $c(0) \neq 0$. We replace c in the sum by $c(x^{-1})x^i/c(0)$ and recall that $R(x, c) = c(0)$. The formula quoted now follows from the theory of resultants.

5 Selberg Sums and Metaplectic Groups

The results of Sect. 3 show that there is a large number of relationships between Selberg sums. The results of Anderson, Evans, and v. Wamelen show that polynomials with two rational zeros over $\mathbf{F}_q$ can be evaluated explicitly. It turns out, as we shall see in the next section, that if the zeros are no longer rational a similar formula holds. The next case which one can investigate, as in [11], is that of polynomials with three rational zeros. In view of Theorem 1 these can be brought to the form $x^{e_0}(x-1)^{e_1}(x-\lambda)^{e_\lambda}$. As in [11] there are a large number of relations between these, now a little more complicated as we have to move into the region of stability. They are the analogues of the relations between such sums similar to transformations of hypergeometric functions (cf. [17, Chap. XIV]). We should note that in this standard form such Selberg sums can be easily computed as the resultant can be evaluated by a continued-fraction type of recursion. This is implemented in, for example, the gp/PARI package. I hope to discuss the results of these calculations in a future paper.

There are some further relations that are of interest. Let n, n' be as in Sect. 3. If $n'|n$ then the generating series

$$\sum_{\substack{i\equiv i_0 \pmod n \\ i\geq 0}} Se(r,\chi_1,\chi_2,i)T^{(i-i_0)/n}$$

which converges in $|T| < q^{-n}$, is, for each $i_0 : 0 \leq i < n$, a rational function in T. There is at most one singularity in $|T| < q^{-n/2}$ and this, if it exists, is simple and is located at $T = q^{-1}(-\tau(\chi_2^{-1}))^{-n}$. These are the series investigated in [10] and [11]. The determination of the residue and the establishing of its properties is one of the major questions addressed in those papers and it is one that has, as yet, only been partially answered.

If the condition $n'|n$ is not satisfied then the series above can also be investigated by means of the theory of Eisenstein series. The point here is that one has to use an Eisenstein series of a "Nebentypus" depending on χ_1 and χ_2. The general theory in contained in [8]. In fact in this case the constant terms of the Eisenstein series will be made up from holomorphic L-series. The analytic continuation then follows from the "principle of the constant term"; see [9, Theorem 4.8] for a statement and [7, Theorem 1.6.6] for a proof in the function-field case. The details have not been given explicitly but it seems very plausible that in this case one will be able to conclude that the series above also in this case represents a rational function but one now with no singularities in $|T| < q^{-n/2}$. One expects that one will be able to determine the denominator and to estimate the degree of the numerator which are known in the metaplectic case also in the non-metaplectic case.

It is instructive to examine the special case $n = 1$. There are two cases, the metaplectic case in which $\chi_1(r/\cdot)$ is a principal character and the other case when $\chi_1(r/\cdot)$ is non-principal. In the first case we see that $\sum_{i\geq 0} Se(r,\chi_1,\chi_2,i)T^i$ is

$L(s, \chi_1(r/\cdot)^{-1}$ with $T = q^{-s}$. Let r_0 be the modulus of $\chi_1(r/\cdot)$; then this series is equal to

$$(1 - q^{1-s}) \prod_{\pi | r_0} (1 - q^{-\deg(\pi)s}).$$

In this case the generating series is a polynomial.

If $\chi_1(r/\cdot)$ is non-principal then, if we suppose for the moment that the $\chi_1(r/\cdot)$ is primitive. Then Anderson, [1], has observed that $L(s, \chi_1(r/\cdot)$ is a polynomial in q^{-s} of degree $\deg(r_0) - 1$. It follows that $L(s, \chi_1(r/\cdot)^{-1}$ has this number of singularities, counted with multiplicities. They lie on $q^{-s} = q^{-1/2}$ by Weil's theorem. If the character is not primitive then there is a numerator of the form $\prod(1 - q^{-s\deg(\pi)})$ where the product is over all the primes dividing the modulus but not the conductor. In the case of the standard Selberg sums the degree of π is 1 and it is of the form $1 - \alpha q^{-s}$ where α is a Jacobi sum. The cases of other r will be much less straightforward.

We return to the general case. The singularities of the generating series of the sequence $Se(r, \chi_1, \chi_2, i)$ are given as certain sums of their coefficients, i.e., of Selberg sums. This has been described in [10, 11]. The theory of metaplectic groups then leads to a number of relations between the residues, the so-called Hecke relations. A consequence of this is that there are a number of unexpected relations between Selberg sums. Some examples are given in [10, Sect. 4]. To date there is no systematic method of treating these relationships. This is not unlike the situation in the theory of generalized hypergeometric functions.

It is interesting to consider Anderson's method in this connection. His approach is based on a formula which is derived from the theory of Dirichlet series over R. We shall now sketch his technique. Let f be a monic polynomial in R. Let χ be as before and let n be its order. We regard $\chi(f/\cdot)$ as a Dirichlet character. Let f_o be the conductor of f. This is $\prod \pi$ where π runs through those monic prime divisors of f whose order in f is not divisible by n. We shall assume that $f_o \neq 1$. Then by [1, Proposition 2.1]

$$\omega(D(f_o))\chi(f/f_o')\tau(\chi^{-1})^{\deg(f)-1} \prod_{\pi | f_o} \tau(\chi^{-\mathrm{ord}_\pi(f)})^{-\deg(\pi)}$$

is equal to

$$\sum_{\substack{g:\deg(g)=\deg(f_o)-1 \\ g \text{ monic}}} \chi(f/g).$$

This is proved by using the functional equation for the L-function $L(s, \chi(f/\cdot))$ and the fact that the latter is a polynomial to determine the coefficient of $(q^{-s})^{\deg(f_o)-1}$. Anderson proves this in the case $n = q - 1$ but the proof is valid whenever $\chi(f/\cdot)$ is not principal. Anderson achieves the same generality through his parameter c.

Anderson's proof of the formula for the Selberg sum exploits the evaluation of a double sum in two different ways. The argument is strongly reminiscent of the multiple Dirichlet series technique, as used, for example, in [3]. The crucial point of the argument is that r_o should be quadratic and it follows that one can also evaluate Selberg sums explicitly when r is a power of an irreducible quadratic polynomial.

It seems plausible that one could use Anderson's method combined with elementary considerations to determine the properties of metaplectic Eisenstein series over rational function fields. In fact the "principle of the constant term" referred to above is relatively elementary and as the constant term is easy to study in this case even the Eisenstein series approach is relatively elementary. The method of multiple Dirichlet series is, at least for higher ranks, an important component in the study of Eisenstein series and so the applicability of both methods should not be surprising. At any rate it should reassure those unfamiliar with this theory that the method is, at heart, in this case at least, elementary.

References

1. G.W. Anderson, The evaluation of Selberg sums. C. R. Acad. Sci. Paris Ser. I **311**, 469–472 (1990)
2. D. Carmon, Z. Rudnick, The autocorrelation function of the Möbius function and Chowla's conjecture for the ration function field. Q. J. Math. **65**, 53–61 (2014)
3. G. Chinta, J.B. Mohler, Sums of *L*-functions over rational function fields. Acta Arith. **144**, 53–68 (2010)
4. K. Conrad, Irreducible values of polynomials: a non-analogy, in *Number Fields and Function Fields – Two Parallel Worlds* (Birkhäuser, Boston, 2005), pp. 71–86
5. R.J. Evans, Identities for products of Gauss sums over finite fields. L'Enseign. Math. **27**, 197–209 (1981)
6. R.J. Evans, The evaluation of Selberg character sums. L'Enseign. Math. **37**, 235–248 (1991)
7. G. Harder, Chevalley groups over function fields and automorphic forms. Ann. Math. **100**, 249–306 (1974)
8. D.A. Kazhdan, S.J. Patterson, Metaplectic forms. Publ. Math. IHES **59**, 35–142 (1984)
9. L.E. Morris, Eisenstein series for reductive groups over global function fields part I: the cusp form case. Can. J. Math. **34**, 91–168 (1982)
10. S.J. Patterson, Note on a paper of J. Hoffstein. Glasgow Math. J. **296**, 125–161, 217–220 (2007)
11. S.J. Patterson, The Fourier coefficients of metaplectic theta series on *GL*(2) over rational function fields. arXiv 1411.7594 (2014)
12. A. Selberg, *Collected Papers, 1* (Springer, Berlin, 1989)
13. R.G. Swan, Factorization of polynomials over finite fields. Pac. J. Math. **12**, 1099–1106 (1962)
14. B.L. van der Waerden, *Modern Algebra* (Trans. F. Blum), vol. 1 (Fredrick Unger Publishing, New York, 1949)
15. P.B. van Wamelen, Proof of the Evans-root conjectures for Selberg character sums. J. Lond. Math. Soc. Ser. II. **48**, 415–426 (1993)
16. A. Weil, *Basic Number Theory* (Springer, Berlin, 1967)
17. E.T. Whittaker, G.N. Watson, *Modern Analysis*, 4th edn. (Cambridge University Press, Cambridge, 1946)

Polignac Numbers, Conjectures of Erdős on Gaps Between Primes, Arithmetic Progressions in Primes, and the Bounded Gap Conjecture

János Pintz

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract In the present work we prove a number of results about gaps between consecutive primes. The proofs need the method of Y. Zhang which led to the proof of infinitely many bounded gaps between primes. Several of the results refer to the so-called Polignac numbers which we define as those even integers which can be written in infinitely many ways as the difference of two consecutive primes. Others refer to several 60–70 years old conjecture of Paul Erdős about the distribution of the normalized gaps between consecutive primes and about the distribution of the ratio of consecutive primegaps. The methods involve an extended version of Zhangs method, a property of the GPY weights proved by the author a few years ago and other ideas as well.

Keywords Gaps between primes • Polignac conjecture • Polignac numbers

2010 Mathematics subject classification: Primary 11N05; Secondary 11N36

1 Introduction

1.1. Recently Yitang Zhang proved the Bounded Gap Conjecture, a term formulated in recent works of mine, often in collaboration with D. Goldston and C. Yıldırım. Let p_n denote the nth prime, $\mathcal{P}$ the set of all primes and

$$d_n = p_{n+1} - p_n \tag{1.1}$$

the nth difference between consecutive primes.

J. Pintz (✉)
Rényi Mathematical Institute of the Hungarian Academy of Sciences,
Reáltanoda u. 13–15, H-1053 Budapest, Hungary
e-mail: pintz@renyi.hu

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_22

Theorem A (Zhang [28]) $\liminf_{n\to\infty} d_n \le 7\cdot 10^7$.

Earlier, in a joint work with D. Goldston and C. Yıldırım we showed [11] this under the deep unproved condition that primes have a distribution level greater than $1/2$, in other words, under the assumption that the exponent $1/2$ in the Bombieri–Vinogradov Theorem can be improved.

Theorem B (Goldston et al. [11]) *If the primes have a distribution level $\vartheta > 1/2$, then with a suitable explicit constant $C(\vartheta)$ we have*

$$\liminf_{n\to\infty} d_n \le C(\vartheta). \tag{1.2}$$

If the Elliott–Halberstam Conjecture (EH) is true, i.e. $\vartheta = 1$ or, at least, $\vartheta > 0.971$, then

$$\liminf_{n\to\infty} d_n \le 16. \tag{1.3}$$

We say that ϑ is a level of distribution of primes if

$$\sum_{q\le X^{\vartheta-\varepsilon}} \max_{\substack{a\\(a,q)=1}} \left| \sum_{\substack{p\equiv a \pmod q\\ p\le X}} \log p - \frac{X}{\varphi(q)} \right| \ll_{A,\varepsilon} \frac{X}{(\log X)} \tag{1.4}$$

for any $A, \varepsilon > 0$. The Bombieri–Vinogradov Theorem asserts that $\vartheta = 1/2$ is a level of distribution and the Elliott–Halberstam Conjecture [4] asserts that $\vartheta = 1$ is also an admissible level.

Somewhat later, in a joint work with Motohashi [19] we showed that in order to reach infinitely many bounded gaps between primes it is sufficient to show (1.4) for smooth moduli q, i.e. with moduli without any prime divisor $> X^b$, where b can be chosen as an arbitrarily fixed constant.

Zhang proved that (1.4) holds for smooth moduli with a $\vartheta > 1/2$ and consequently obtained Theorem A. (We have to mention that he did not mention our work [19] in his paper at all despite our notice, instead he published his proof of our result.)

The present paper is a modified version of the author's preprint of 27 May 2013 (available at arXiv:1305.6289v1) written before the alternative proofs of the Bounded Gap Conjecture by Maynard [18] and Tao (unpublished) and it contains several results which can be reached by using (1.4) for smooth moduli with any $\vartheta > 1/2$ and among others ideas of the author from [20]. Several of these results (sometimes in modified forms) were mentioned in the author's lecture in Hildesheim, in July of 2014.

We mention that the method of Maynard–Tao led later to several similar results as our present ones (often coupled with other ideas, and often in stronger forms as well, although they might be weaker in some other sense).

2 History of the Problems: Formulation of the Results

2.1 Approximations to the Twin Prime Conjecture

The problem of finding small gaps between primes originates from the

Twin Prime Conjecture $\liminf_{n\to\infty} d_n = 2$.

Since by the prime number theorem the average gap size is $\log n$, Hardy and Littlewood considered first already in 1926 in an unpublished manuscript (see, however [23]) the upper estimation of

$$\Delta_1 = \liminf_{n\to\infty} \frac{d_n}{\log n} \tag{2.1}$$

and showed $\Delta_1 \le 2/3$ under the assumption of the generalized Riemann hypothesis (GRH).

Erdős [5] was the first to show unconditionally

$$\Delta_1 < 1 - c_0, \quad c_0 > 0 \tag{2.2}$$

with an unspecified but explicitly calculable positive constant c_0. The full history with about 12–15 improvements concerning the value of Δ_1 is contained in [11], so we list here just the most important steps:

$$\Delta_1 < 0.4666 \text{ (Bombieri and Davenport [1])}, \tag{2.3}$$

$$\Delta_1 < 0.2485 \text{ (Maier [17])}. \tag{2.4}$$

This was the best result until 2005 when we showed in a joint work with D. Goldston and C. Yıldırım what we called the small gap conjecture:

Theorem A (Goldston et al. [11]) $\Delta_1 = 0$.

Soon after it we improved this to

Theorem B (Goldston et al. [12]) *We have*

$$\liminf_{n\to\infty} \frac{d_n}{(\log n)^{1/2}(\log\log n)^2} < \infty. \tag{2.5}$$

Finally a few years ago I improved the exponent to $3/7$ and announced the result at the Journées Arithmétiques, Vilnius, 2011, and Turán Memorial Conference, Budapest, 2011.

Theorem C (Pintz [22])

$$\liminf_{n\to\infty} \frac{d_n}{(\log n)^{3/7}(\log\log n)^{4/7}} < \infty. \tag{2.6}$$

In a joint work with Farkas et al. [9] we also showed that essential new ideas are necessary to improve (2.6).

2.2 Polignac Numbers

The twin prime conjecture appeared already in a more general form in 1849 in a work of de Polignac.

First we give two definitions.

Definition D A positive even number $2k$ is a strong Polignac number, or briefly a Polignac number if $d_n = 2k$ for infinitely many values of n.

Definition E A positive even number $2k$ is a weak Polignac number if it can be written as the difference of two primes in an infinitude of ways.

The set of (strong) Polignac numbers will be denoted by $\mathcal{D}_s$, the set of weak Polignac numbers by $\mathcal{D}_w$. (We have trivially $\mathcal{D}_s \subseteqq \mathcal{D}_w$.)

Polignac's Conjecture (de Polignac [2]) Every positive even integer is a (strong) Polignac number.

Since the smallest weak Polignac number has to be a strong Polignac number, an easy consideration gives that using $|A|$ (or sometimes $\#A$) to denote the number of elements of a set A, the following proposition is true.

Proposition The following three statements are equivalent:

(i) the bounded gap Conjecture is true;
(ii) there is at least one (strong) Polignac number, i.e. $|\mathcal{D}_s| \geq 1$;
(iii) there is at least one weak Polignac number, i.e. $|\mathcal{D}_w| \geq 1$.

The above very simple proposition shows that the bounded gap conjecture itself leaves still many problems open about Polignac numbers or weak Polignac numbers, but solves the crucial problem that their set is nonempty. We will prove several unconditional results about the density and distribution of (strong) Polignac numbers.

Theorem 2.6 *There exists an explicitly calculable constant c such that for $N > N_0$ we have at least cN Polignac numbers below N, i.e. Polignac numbers have a positive lower asymptotic density.*

Theorem 2.7 *There exists an ineffective constant C' such that every interval of type $[M, M + C']$ contains at least one Polignac number.*

Remark As mentioned earlier, the term Polignac number means always strong Polignac numbers.

2.3 The Normalized Value Distribution of d_n

The prime number theorem implies

$$\lim_{N\to\infty}\frac{1}{N}\sum\frac{d_n}{\log n}=1, \tag{2.7}$$

so it is natural to investigate the series $d_n/\log n$. Denoting by J the set of limit points of $d_n/\log n$, Erdős [7] conjectured

$$J=\left\{\frac{d_n}{\log n}\right\}'=[0,\infty]. \tag{2.8}$$

While Westzynthius [27] proved more than 80 years ago that $\infty\in J$, no finite limit point was known until 2005 when we showed the small gap conjecture, i.e. Theorem A [11], which is equivalent to $0\in J$.

Interestingly enough Erdős [7] and Ricci [24] proved independently about 60 years ago that J has a positive Lebesgue measure. What I can show is a weaker form of Erdős's conjecture (2.8).

Theorem 2.8 *There is an ineffective constant $c>0$ such that*

$$[0,c]\subset J. \tag{2.9}$$

Kálmán Győry asked me at the Turán Memorial Conference in Budapest, 2011 whether it is possible to find a form of the above result which gives answers about the more subtle value-distribution of d_n if we use a test-function $f(n)\le\log n$, $f(n)\to\infty$ as $n\to\infty$.

Definition 2.9 Let $\mathcal{F}$ denote the class of functions $f:\mathbb{Z}^+\to R^+$ with a slow oscillation, when for every $\varepsilon>0$ we have an $N(\varepsilon)>0$ such that

$$(1-\varepsilon)f(N)\le f(n)\le(1+\varepsilon)f(N)\ \text{ for }\ N\le n\le 2N,\quad N>N(\varepsilon). \tag{2.10}$$

Theorem 2.10 *For every function $f\in\mathcal{F}$, $f(n)\le\log n$, $\lim_{n\to\infty}f(n)=\infty$ we have an ineffective constant $c_f>0$ such that*

$$[0,c_f]\subset J_f:=\left\{\frac{d_n}{f(n)}\right\}'. \tag{2.11}$$

2.4 Comparison of Two Consecutive Values of d_n

Erdős and Turán proved 65 years ago [8] that $d_{n+1}-d_n$ changes sign infinitely often. This was soon improved by Erdős [6] to

$$\liminf_{n\to\infty}\frac{d_{n+1}}{d_n} < 1 < \limsup_{n\to\infty}\frac{d_{n+1}}{d_n}. \tag{2.12}$$

Erdős [7] wrote 7 years later: "One would of course conjecture that

$$\liminf_{n\to\infty}\frac{d_{n+1}}{d_n} = 0, \quad \limsup_{n\to\infty}\frac{d_{n+1}}{d_n} = \infty, \tag{2.13}$$

but these conjectures seem very difficult to prove."

In Sect. 6 I will show this in a much stronger form:

Theorem 2.11 *We have*

$$\liminf_{n\to\infty}\frac{d_{n+1}/d_n}{(\log n)^{-1}} < \infty \tag{2.14}$$

and

$$\limsup_{n\to\infty}\frac{d_{n+1}/d_n}{\log n} > 0. \tag{2.15}$$

2.5 Arithmetic Progressions in the Sequence of Generalized Twin Primes

Based on the method of Vinogradov [26] van der Corput [25] showed the existence of infinitely many 3-term arithmetic progressions in the sequence of primes. The problem of the existence of infinitely many k-term arithmetic progressions was open for all $k \geq 4$ until 2004, when Green and Tao [14] found their wonderful result that primes contain k-term arithmetic progressions for every k. I found recently [20] a common generalization of Green–Tao's result and our Theorem B [12] under the deep assumption that there is a level $\vartheta > 1/2$ of the distribution of primes. Combining Zhang's method with that of [20] I can prove now the following:

Theorem 2.12 *There is a $d \leq 7\times 10^7$ such that there are arbitrarily long arithmetic progressions of primes with the property that $p' = p + d$ is the prime following p for each element of the progression.*

3 Preparation for the Proofs

All the proofs use some modified form of the conjecture of Dickson [3] about k-tuples of primes. (His original conjecture referred for linear forms with integer coefficients.) Let $\mathcal{H} = \{h_i\}_{i=1}^{k}$ be a k-tuple of different non-negative integers. We call $\mathcal{H}$ admissible, if

$$P_{\mathcal{H}}(n) = \prod_{i=1}^{k}(n - h_i) \tag{3.1}$$

has no fixed prime divisor, that is, if the number $\nu_p(\mathcal{H})$ of residue classes covered by $\mathcal{H}$ mod p satisfies

$$\nu_p(\mathcal{H}) < p \quad \text{for} \quad p \in \mathcal{P}. \tag{3.2}$$

This is equivalent to the fact that the singular series

$$\mathfrak{S}(\mathcal{H}) = \prod_{p}\left(1 - \frac{\nu_p(\mathcal{H})}{p}\right)\left(1 - \frac{1}{p}\right)^{-k} > 0. \tag{3.3}$$

Dickson conjectured that if $\mathcal{H}$ is admissible, then all $n + h_i$ will be primes simultaneously for infinitely many values of n.

Hardy and Littlewood [16], probably unaware of Dickson's conjecture, formulated a quantitative version of it, according to which

$$\pi_{\mathcal{H}}(x) = \sum_{\substack{n \le x \\ n+h_i \in \mathcal{P}(1 \le i \le k)}} 1 = \big(\mathfrak{S}(\mathcal{H}) + o(1)\big)\frac{x}{\log^k x}. \tag{3.4}$$

In the work [11] we attacked (but missed by a hair's breadth) the following weaker form of Dickson's conjecture which I called

Conjecture DHL $(k, 2)$ If $\mathcal{H}$ is an admissible k-tuple, then $n + \mathcal{H}$ contains at least two primes for infinitely many values of n.

It is clear that if DHL$(k, 2)$ is proved for any k (or even for any single k-tuple $\mathcal{H}_k$), then the Bounded Gap Conjecture is true. DHL$(k, 2)$ was shown very recently by Zhang [28] for $k \ge k_0 = 3.5 \times 10^6$ and this implied his Theorem A, the infinitude of gaps of size $\le 7 \cdot 10^7$.

However, results of this type cannot exclude the existence of other primes and therefore give information on numbers expressible as difference of two primes, in the optimal case of Zhang's very strong Theorem A prove the existence of many weak Polignac numbers. However, they do not provide more information about (strong) Polignac numbers than the very deep fact that $\mathcal{D}_s \neq \emptyset$ and they do not help in showing any of Theorems 2.6–2.12. For example, in case of Theorem 2.12 they do not yield, let say, 4-term arithmetic progressions of primes and a bounded number d

such that $p + d$ should also be prime for all four elements of the progression (even if we do not require that p and $p + d$ should be *consecutive* primes).

By a combination of the ideas of D. Goldston, C. Yıldırım, Y. Zhang and mine, I am able to show a much stronger form of Conjecture DHL$(k, 2)$ which may be applied towards the proof of Theorems 2.6–2.12. In case of Theorem 2.12 the ground-breaking ideas of Green and Tao [14] have to be used too, of course.

In view of Zhang's recent result the stronger form of Conjecture DHL$(k, 2)$ (to be proved below) will be called Conjecture DHL$^*(k, 2)$.

Let $P^-(m)$ denote the smallest prime factor of m.

Conjecture DHL* $(k, 2)$ Let $k \geq 2$ and $\mathcal{H} = \{h_i\}_{i=1}^k$ be any admissible k-tuple, $N \in Z^+$, $\varepsilon > 0$ sufficiently small $(\varepsilon < \varepsilon_0)$

$$\mathcal{H} \subset [0, H], \quad H \leq \varepsilon \log N, \quad P_{\mathcal{H}}(n) = \prod_{i=1}^{k}(n + h_i). \tag{3.5}$$

We have then positive constants $c_1(k)$ and $c_2(k)$ such that the number of integers $n \in [N, 2N)$ such that $n + \mathcal{H}$ contains at least two *consecutive* primes and almost primes in each components (i.e. $P^-(P_{\mathcal{H}}(n)) > n^{c_1(k)}$) is at least

$$c_2(k)\mathfrak{S}(\mathcal{H})\frac{N}{\log^k N} \quad \text{for } N > N_0(\mathcal{H}). \tag{3.6}$$

One can see that we have a looser condition than in DHL$(k, 2)$ as far as the elements of $\mathcal{H}$ are allowed to tend to infinity as fast as $\varepsilon \log N$. On the other hand, we get stronger consequences as

1. we can prescribe that the two primes $n + h_i$ and $n + h_j$ in our k-tuple should be *consecutive*;
2. we have almost primes in each component $n + h_i$;
3. we get the lower estimate (3.6) for the number of the required n's with the above property.

The condition $n \in [N, 2N)$ makes usually no problem but in case of the existence of Siegel zeros some extra care is needed if we would like to have effective results (see Sect. 8 for this).

After this it is easy to formulate (but not to prove) our

Main Theorem Conjecture DHL$^*(k, 2)$ is true for $k \geq 3.5 \times 10^6$.

Proof Since this result contains Zhang's Theorem and even more, it is easy to guess that a self-contained proof would be hopelessly long (and difficult). We therefore try to describe only the changes compared to different earlier works.

The first pillar of Zhang's work is the method of proof of our Theorem B. Although he supposes $\mathcal{H}$ as a constant the method of proof of Theorem B (see Propositions 1 and 2 in [11]) allows beyond $H \ll \log N$ (required by (3.5) above) the much looser condition $H \ll N^{1/4-\varepsilon}$ for any $\varepsilon > 0$.

The second pillar of Zhang's work is to show that distribution of primes according to non-smooth moduli, i.e. with some prime divisor $> N^b$ for any fixed small constant b, can be neglected. As mentioned in the Introduction we showed this already much earlier in a joint work with Motohashi [19]. This work also supposed $\mathcal{H}$ to be a constant but the only place where actually more care is needed in the proof is (3.11) of [19]. On the other hand, allowing here the condition

$$H \ll \log N, \tag{3.7}$$

the same simple argument as in Sect. 6 of [11] adds an additional error term

$$k^2 \log\log\log R \ll \log\log\log R \tag{3.8}$$

to the right-hand side of (3.11) of [19] which is far less than the present error term $\log R_0 = \log R/(\log\log R)^5$. Otherwise the proof works without any change, everything remains uniform under our condition (3.7) above.

Remark The crucial Lemmas 3 and 4 of our work [19] contain an additional factor $\gamma(n, \mathcal{H})$. However, by the definition (4.17) of [19] we have $\gamma(n, \mathcal{H}) = 1$ if $P^-\big(P_{\mathcal{H}}(n)\big) > R^\eta$ for any fixed $\eta > 0$. In such a way the extra factor $\gamma(n, \mathcal{H})$ does not affect the validity of our Lemma 3.2 below since the asymptotic provided by Lemma 3.3 for the right-hand side of (3.11) (and similarly the analogue of it for primes, Lemma 3.4) is the same as if we used the constant weight 1 instead of $\gamma(n, \mathcal{H})$.

No change is required in the third pillar of Zhang's work where he proves some sort of extension of the Bombieri–Vinogradov theorem for smooth moduli and the residue classes appearing by the method of Theorem B.

However, the proof of Theorem DHL$^*(k, 2)$ (for k large enough, $k \geq 3.5 \cdot 10^6$) requires a further important idea, namely Lemmas 3–4 of the author's work [20]. This we formulate now as

Lemma 3.1 *Let $N^{c_0} < R \leq \sqrt{N/p}(\log N)^{-C}$, $p \in \mathcal{P}$, $p < R^{c_0}$ with a sufficiently small positive c_0 and sufficiently large C. Then we have with the notation*

$$\Lambda_R(n; \mathcal{H}, k+\ell) = \frac{1}{(k+\ell)!} \sum_{d \leq R, d \mid P_{\mathcal{H}}(n)} \mu(d) \left(\log \frac{R}{d}\right)^{k+\ell} \quad (\ell \leq k) \tag{3.9}$$

the relation

$$\sum_{\substack{n \in [N, 2N) \\ p \mid P_{\mathcal{H}}(n)}} \Lambda_R(n; \mathcal{H}, k+\ell)^2 \ll_k \frac{\log p}{p \log R} \sum_{n \in [N, 2N)} \Lambda_R(n; \mathcal{H}, k+\ell)^2. \tag{3.10}$$

Lemma 3.1 immediately implies

Lemma 3.2 *Let* $N^{c_0} < R \le N^{1/(2+\eta)}(\log N)^{-C}, \quad \eta > 0$. *We have then*

$$\sum_{\substack{n\in[N,2N)\\ P^-(P_{\mathcal{H}}(n))<R^\eta}} \Lambda_R(n;\mathcal{H},k+\ell)^2 \ll_k \eta \sum_{n\in[N,2N)} \Lambda_R(n;\mathcal{H},k+\ell)^2. \tag{3.11}$$

Remark Lemmas 3.1 and 3.2 were already proved in [20] under the loose condition $H \ll \log N$.

Lemma 3.2 asserts that numbers n where $P_H(n)$ has a prime factor $< R^\eta$ (equivalently $< N^b$) with a small enough value of η (or b) might be neglected, since the weight used in all proofs is actually of type (3.9). The value of η (or b) depends on k.

These results play a crucial role in the common generalization of the Green–Tao theorem and of our Theorem B (cf. [20]) and also in the proof that prime gaps $< \varepsilon \log p$ form a positive proportion of all gaps for any $\varepsilon > 0$ (proved in a joint work with Goldston and Yıldırım).

These four pillars lead finally to the stronger form of Theorem DHL$^*(k,2)$ if we combine it with a standard assertion following from Selberg's sieve, which we can formulate in this special case as

Lemma 3.3 *Let* $0 < \alpha < 1/2$ *be any constant. Then*

$$\sum_{\substack{n\in[N,2N)\\ P^-(P_{\mathcal{H}}(n))>N^\alpha}} 1 \ll_k \frac{N\alpha^{-k}}{\log^k N}\mathfrak{S}(\mathcal{H}). \tag{3.12}$$

Proof This is Theorem 5.1 of [15] or Theorem 2 in Sect. 2.2.2 of [13]. This is also valid if we assume only $H \ll \log N$.

We further need a generalization of Gallagher's theorem proved by the author which we formulate as

Lemma 3.4 *Let* $\mathcal{H}_k$ *be an arbitrary admissible* k*-tuple with*

$$\mathcal{H} = \mathcal{H}_k \subseteqq [0,H]. \tag{3.13}$$

Then we have for any $\eta > 0$

$$S_{\mathcal{H}}(H) := \frac{1}{H}\sum_{h=1}^{H} \frac{\mathfrak{S}(\mathcal{H}\cup h)}{\mathfrak{S}(\mathcal{H})} = 1 + O(\eta) \tag{3.14}$$

if

$$H \ge \exp(k^{1/\eta}). \tag{3.15}$$

Proof This is Theorem 1 of [21].

Remark As it is easy to see Lemma 3.4 implies Gallagher's classical theorem [10] on the singular series.

Combining the proofs of Theorems A and B (in the modified forms mentioned above) with the assertion of Lemma 3.2 we obtain under the weaker condition (3.6), i.e. for all admissible k-tuples $\mathcal{H}_k = \{h_i\}_{i=1}^k$, $h_i < h_{i+1}$,

$$\mathcal{H} = \mathcal{H}_k \subseteqq [0, \varepsilon \log N], \tag{3.16}$$

at least

$$c_2(k)\mathfrak{S}(\mathcal{H})\frac{N}{\log^k N} \tag{3.17}$$

numbers $n \in [N, 2N)$ such that $n+\mathcal{H}$ contains at least two primes and almost primes in each components, i.e.

$$P^-\big(P_{\mathcal{H}}(n)\big) > n^{c_1(k)}. \tag{3.18}$$

However, we must show the same with *consecutive* primes as well.

We can define for any subset V of $\{1, 2, \dots, k\}$ the set

$$V(N) = \big\{n \in [N, 2N) :\ n + h_i \in \mathcal{P} \Leftrightarrow i \in V\big\}. \tag{3.19}$$

Since k is bounded the number of possible subsets V is also bounded, therefore we can choose a V_0 such that

$$V_0 \subset \{1, 2, \dots, k\}, \quad |V_0| \geq 2, \quad |V_0(N)| \geq c_3(k)\mathfrak{S}(\mathcal{H})\frac{N}{\log^k N}. \tag{3.20}$$

Choosing two arbitrary consecutive elements $i, j \in V_0(N)$ with $i < j$ we have at least

$$c_3(k)\mathfrak{S}(\mathcal{H})\frac{N}{\log^k N} \tag{3.21}$$

numbers $n \in [N, 2N)$ such that for any $\mu \in (i, j)$

$$n + h_\mu \notin \mathcal{P}. \tag{3.22}$$

We have to assure, however, additionally that for a positive proportion of these numbers n we have also

$$n + h \notin \mathcal{P} \ \text{ for } \ h \notin \mathcal{H}, \ \ h_i < h < h_j. \tag{3.23}$$

Applying Lemma 3.3 for all these values h and summing up we arrive at the conclusion that

$$\sum_{\substack{n\in[N,2N)\\ P^-(P_{\mathcal{H}}(n))>N^{c_1(k)}}} \sum_{\substack{h\\ h_i<h<h_j\\ n+h\in\mathcal{P}}} 1 \le C_4(k)\frac{N}{\log^{k+1}N}\sum_{h_i<h<h_j}\mathfrak{S}(\mathcal{H}\cup h) \tag{3.24}$$

$$\le 2C_4(k)\frac{N\varepsilon\mathfrak{S}(\mathcal{H})}{\log^k N}$$

by Lemma 3.4. This shows that if ε was chosen sufficiently small depending on k, i.e.

$$\varepsilon < \varepsilon_0(k) \tag{3.25}$$

then our original primes $n + h_i$ and $n + h_j$ are *consecutive* for at least

$$c_5(k)\mathfrak{S}(\mathcal{H})\frac{N}{\log^k N} \tag{3.26}$$

elements $n \in [N, 2N)$, thereby showing our Main Theorem.

4 Polignac Numbers

Proof of Theorem 2.6

The fact that DHL$^*(k, 2)$ implies the positivity of the asymptotic lower density of Polignac numbers is expressed as Corollary 1 of [20] with the value

$$\frac{1}{k(k-1)}\prod_{p\le k}\left(1-\frac{1}{p}\right) \tag{4.1}$$

and proved in Sect. 11 of [20]. The above value is about $e^{-\gamma}/(k^2\log k)$ for large values of k. (If $k \to \infty$, they are asymptotically equal.)

Proof of Theorem 2.7

We again suppose DHL$^*(k, 2)$ for $k \ge k_0$.

The reasoning is more intricate in this case and the resulting value C is ineffective. The trivial relation

$$h_k - h_1 \ge (k-1)\min_{i>j}(h_i - h_j) \quad (h_i < h_{i+1}) \tag{4.2}$$

even gives the impression that the best we can prove about localization of Polignac numbers is an interval of type

$$\big[M, (k-1)M\big]. \tag{4.3}$$

Let us suppose that Theorem 2.7 is false. Then we have for any $C_0 > 0$ an infinite series of intervals

$$I_\nu := \big[M_\nu, M_\nu + C_\nu\big], \quad M_\nu > C_\nu > 4M_{\nu-1}, \quad M_1 > C_0 \tag{4.4}$$

such that

$$\mathcal{D}_s \cap \left(\bigcup_{\nu=1}^{\infty} I_\nu\right) = \emptyset. \tag{4.5}$$

For $p > k$ we have clearly

$$v_p(\mathcal{H}_k) < p \ \text{ for } \ p \in \mathcal{P}, \tag{4.6}$$

so we have no problem of choosing an admissible system $\mathcal{H}_k$ in a sufficiently long interval (e.g. if C_k is large enough). Let

$$\mathcal{H}_k := \{h_\nu\}_{\nu=1}^{k}, \quad h_\nu \in I'_\nu := \big[M_\nu + C_\nu/2, M_\nu + C_\nu\big]. \tag{4.7}$$

For $h_\nu \in I_\nu$, $h_\mu \in I_\mu$, $\nu < \mu$ we have then

$$h_\mu - h_\nu \in \big[M_\mu + C_\mu/2 - 2M_{\mu-1}, M_\mu + C_\mu\big] \subset I_\mu. \tag{4.8}$$

Since in case of $k \geq k_0$ at least one of the numbers

$$h_\mu - h_\nu \qquad (1 \leq \nu < \mu \leq k) \tag{4.9}$$

can be written as a difference of two consecutive primes, (4.8) contradicts to (4.5) and thus proves our theorem.

5 The Normalized Value Distribution of d_n

Proof of Theorems 2.8–2.10

Since Theorem 2.10 implies Theorem 2.8 it is sufficient to prove the latter. The structure of the proof will follow that of Theorem 2.7 proved in the previous section. Suppose that Theorem 2.10 is false. In this case we have for a sufficiently small

$c^* > 0$ an infinite series of intervals

$$J_\nu = \big[c_\nu, c_\nu + \delta_\nu\big], \quad c_\nu > 4\delta_\nu > 20c_{\nu+1}, \quad c_1 < c^* \tag{5.1}$$

such that for K large enough

$$\left\{\frac{d_n}{f(n)}\right\}_{n=N}^{\infty} \cap \left(\bigcup_{\nu=1}^{K} J_\nu\right) = \emptyset, \text{ where } N = N(K) > 0. \tag{5.2}$$

Let

$$I_\nu(n) := \big[c_\nu f(n), (c_\nu + \delta_\nu)f(n)\big], \quad \nu = 1, 2, \dots, K. \tag{5.3}$$

Then we have

$$d_n \notin \bigcup_{\nu=1}^{K} I_\nu(n) \text{ for } \nu = 1, 2, \dots, K, \ n \in [N, 2N), \ N > N(k). \tag{5.4}$$

Using our Main Theorem, similarly to (4.7) we can construct an admissible k-tuple $\mathcal{H}_k = \{h_\nu\}_{\nu=1}^{k}$ with $3.5 \cdot 10^6 \le k \le K$ such that $h_1 > h_2 > \cdots > h_k$ and with a sufficiently small $\varepsilon > 0$

$$h_\nu \in I'_\nu(N) := \left[\left(c_\nu + \frac{\delta_\nu}{2}\right)(1+\varepsilon)f(N), (c_\nu + \delta_\nu)(1-\varepsilon)f(N)\right]. \tag{5.5}$$

For $h_\mu \in I'_\mu$, $h_\nu \in I'_\nu$, $\mu < \nu$ we have for $N > \max\big(N(K), N_0(\varepsilon)\big)$

$$h_\mu - h_\nu \in \left[\left(c_\mu + \frac{\delta_\mu}{2} - 2c_{\mu+1}\right)(1+\varepsilon)f(N), (c_\mu + \delta_\mu)(1-\varepsilon)f(N)\right] := I^*_\mu(N). \tag{5.6}$$

Since we have for any $1 \le \mu < \nu \le k_0$ and any $n \in [N, 2N)$

$$I^*_\mu(N) \subset I_\mu(n), \tag{5.7}$$

the fact that by the Main Theorem $h_\mu - h_\nu = d_n$ for some $n \in [N, 2N)$, $1 \le \mu < \nu \le k_0$ contradicts to (5.4) and thus proves Theorems 2.8 and 2.10.

6 Comparison of Two Consecutive Values of d_n

Proof of Theorem 2.11

Since the proof of the two inequalities is completely analogous, we will only prove the second one. The basis of it is the Main Theorem proved in Sect. 3. We can

start with an arbitrary admissible k-tuple $\mathcal{H} = \mathcal{H}_k = \{h_i\}_{i=1}^k$, $h_1 < h_2 < \cdots < h_k$ with $k \geq 3.5 \cdot 10^6$. Let with a fixed sufficiently small $c_1(k)$ define

$$B(i,j,N) = \left\{n \leq N, n + h_i \in \mathcal{P}, n + h_j \in \mathcal{P}, \mathcal{P}^-(\mathcal{P}_{\mathcal{H}}(n)) > n^{c_1(k)}\right\}, \tag{6.1}$$

$$\mathcal{T} = \left\{(i,j); j > i, \limsup_{N\to\infty} \frac{|B(i,j,N)| \log^k N}{N} > 0\right\} \tag{6.2}$$

and let us choose the pair (i,j) with maximal value of j, afterwards that with maximal value of $i < j$. Then for any $h_\mu \in (h_i, h_j)$ (i.e. $i < \mu < j$) we have clearly

$$\limsup_{N\to\infty} \frac{|B(\mu,j,N)| \log^k N}{N} = 0 \tag{6.3}$$

so all components $n + h_\mu$ between $n + h_i$ and $n + h_j$ are almost always composite if $n \in B(i,j,N)$ and $N = N_\nu \to \infty$ through a suitable sequence N_ν.

On the other hand, if we have an arbitrary $h \in (h_i, h_j)$, $h \notin \mathcal{H}$, then the assumption $n + h \in \mathcal{P}$ implies for $\mathcal{H}^+ = \mathcal{H} \cup h$

$$P^-\big(P_{\mathcal{H}^+}(n)\big) > n^{c_1(k)}. \tag{6.4}$$

However, by Lemma 3.3 the number of such $n \leq N$ is for all N

$$\ll_{k,c_1} \frac{\mathfrak{S}(\mathcal{H} \cup \{h\})N}{\log^{k+1} N} \ll_{k,c_1} \frac{\mathfrak{S}(\mathcal{H})N \log h_k}{\log^{k+1} N} \ll_{k,c_1,\mathcal{H}} \frac{N}{\log^{k+1} N}. \tag{6.5}$$

This together with (6.3) shows that we have at least

$$\big(c_1(k,\mathcal{H}) + o(1)\big)\frac{N}{\log^k N} \tag{6.6}$$

values $n \leq N$ with $n + h_i$, $n + h_j$ being consecutive primes for some sequence $N = N_\nu \to \infty$.

Let us consider now these differences. Let

$$n + h_i = p_\nu \in \mathcal{P}, \quad n + h_j = p_{\nu+1} \in \mathcal{P}, \quad d_\nu = h_j - h_i \ll 1 \tag{6.7}$$

where

$$\log n \sim \log \nu \sim \log N. \tag{6.8}$$

Suppose now that the second inequality of Theorem 2.11 is false. Then we have for all those values of ν with an arbitrary $\varepsilon > 0$ for $N > N(\varepsilon)$

$$d_{\nu+1} \leq d_\nu \varepsilon \log N \leq C\varepsilon \log N, \quad C = h_k - h_1. \tag{6.9}$$

The already quoted sieve of Selberg (Lemma 3.3) gives an upper estimate how often this might happen for any particular value

$$d_{\nu+1} = d \le C\varepsilon \log N. \tag{6.10}$$

Adding it up until $C\varepsilon \log N$ we obtain at most

$$\ll_{k,c_1} \frac{N}{\log^{k+1} N} \sum_{h=1}^{C\varepsilon \log N} \mathfrak{S}(\mathcal{H} \cup h) \ll_{k,c_1} \mathfrak{S}(\mathcal{H}) \frac{CN}{\log^k N} \varepsilon \tag{6.11}$$

by Lemma 3.4. This means that in view of (6.6) this cannot hold for all $N = N_\nu \to \infty$. This contradiction proves Theorem 2.11.

7 Arbitrarily Long Arithmetic Progressions of Generalized Twin Primes

Proof of Theorem 2.12

In this case we have to use again our crucial Main Theorem and the rest of the machinery executed in Sect. 7 of [20]. This yields the combination of Zhang's theorem with that of Green and Tao [14].

8 How to Make Zhang's Theorem Effective?

Our last point is that in its original form Zhang's theorem is ineffective since it uses Siegel's theorem. His result and similarly to it all results of the present work can be made effective in the following way.

According to the famous theorem of Landau–Page there is at most one real primitive character χ with a modulus q (and the characters induced by it) which might cause ineffectivity in the Bombieri–Vinogradov theorem, and if it causes ineffectivity, then this modulus has to satisfy

$$(\log X)^2 \le q \le (\log X)^{\omega(X)} \tag{8.1}$$

for any $\omega(X) \to \infty$ as $X \to \infty$. This modulus can cause any problem only in the case

$$q \mid P_{\mathcal{H}}(n). \tag{8.2}$$

However, our Lemma 3.3 says that we can neglect all numbers n with

$$P^{-}\left(P_{\mathcal{H}}(n)\right) < n^{c_1(k)}, \tag{8.3}$$

so (prescribing additionally $q \nmid d$ in the definition (3.9) of $\Lambda_R(n; \mathcal{H}, k, \ell)$) both Zhang's theorem and all our present results become effective.

Remark It is an interesting phenomenon that in the sieving process yielding bounded gaps between primes and in all our present results we can choose

$$\lambda_d = 0 \tag{8.4}$$

if d has either a prime divisor

$$> N^{c'(k)} \tag{8.5}$$

or if it has a prime divisor

$$< N^{c''(k)}. \tag{8.6}$$

Acknowledgements The author "János Pintz" is supported by OTKA grants NK 104183, K 100291 and ERC-AdG. 321104.

References

1. E. Bombieri, H. Davenport, Small differences between prime numbers, Proc. R. Soc. Ser. A **293**, 1–18 (1966)
2. A. de Polignac, Six propositions arithmologiques déduites de crible d'Ératosthene. Nouv. Ann. Math. **8**, 423–429 (1849)
3. L.E. Dickson, A new extension of Dirichlet's theorem on prime numbers. Messenger Math. **33**(2), 155–161 (1904)
4. P.D.T.A. Elliott, H. Halberstam, A conjecture in prime number theory, in *Symposia Mathematica*, vol. 4 (INDAM, Rome, 1968/1969) (Academic, London, 1970), pp. 59–72
5. P. Erdős, The difference of consecutive primes. Duke Math. J. **6**, 438–441 (1940)
6. P. Erdős, On the difference of consecutive primes. Bull. Am. Math. Soc. **54**, 885–889 (1948)
7. P. Erdős, Some problems on the distribution of prime numbers. Teoria dei Numeri, Math. Congr. Varenna, 8 pp. (1954/1955).
8. P. Erdős, P. Turán, On some new questions on the distribution of prime numbers. Bull. Am. Math. Soc. **54**, 371–378 (1948)
9. B. Farkas, J. Pintz, Sz. Gy. Révész, On the optimal weight function in the Goldston–Pintz–Yıldırım method for finding small gaps between consecutive primes, in *Turán Memorial, Number Theory, Combinatorics and Analysis* (de Gruyter, Berlin, 2014), pp. 75–104
10. P.X. Gallagher, On the distribution of primes in short intervals. Mathematika **23**, 4–9 (1976)
11. D.A. Goldston, J. Pintz, C. Yıldırım, Primes in tuples. I. Ann. Math. (2) **170**(2), 819–862 (2009)
12. D.A. Goldston, J. Pintz, C. Yıldırım, Primes in tuples. II. Acta Math. **204**(1), 1–47 (2010)
13. G. Greaves, *Sieves in Number Theory* (Springer, Berlin, 2001)

14. B. Green, T. Tao, The primes contain arbitrarily long arithmetic progressions. Ann. Math. (2) **167**(2), 481–547 (2008)
15. H. Halberstam, H.-E. Richert, *Sieve Methods* (Academic Press, London, 1974)
16. G.H. Hardy, J.E. Littlewood, Some problems of 'Partitio Numerorum', III: on the expression of a number as a sum of primes. Acta Math. **44**, 1–70 (1923)
17. H. Maier, Small differences between prime numbers. Mich. Math. J. **35**, 323–344 (1988)
18. J. Maynard, Small gaps between primes, Ann. Math. (2) **181**(1), 383–413 (2015)
19. Y. Motohashi, J. Pintz, A smoothed GPY sieve. Bull. Lond. Math. Soc. **40**(2), 298–310 (2008)
20. J. Pintz, Are there arbitrarily long arithmetic progressions in the sequence of twin primes?, in *An Irregular Mind. Szemerédi is 70.* Bolyai Society Mathematical Studies, vol. 21 (Springer, Berlin, 2010), pp. 525–559
21. J. Pintz, On the singular series in the prime k-tuple conjecture (2010). arXiv: 1004.1084v1 [math.NT]
22. J. Pintz, Some new results on gaps between consecutive primes, in *Turán Memorial, Number Theory, Combinatorics and Analysis* (de Gruyter, Berlin, 2014), pp. 231–247
23. R.A. Rankin, The difference between consecutive prime numbers. II. Proc. Camb. Philos. Soc. **36**, 255–266 (1940)
24. G. Ricci, Sull'andamento della differenza di numeri primi consecutivi. Riv. Mat. Univ. Parma **5**, 3–54 (1954)
25. J.G. van der Corput, Über Summen von Primzahlen und Primzahlquadraten. Math. Ann. **116**, 1–50 (1939)
26. I.M. Vinogradov, Representation of an odd number as a sum of three prime numbers. Dokl. Akad. Nauk. SSSR **15**, 291–294 (1937) (Russian)
27. E. Westzynthius, Über die Verteilung der Zahlen, die zu der n ersten Primzahlen teilerfremd sind. Commun. Phys. Math. Helsingfors (5) **25**, 1–37 (1931)
28. Y. Zhang, Bounded gaps between primes. Ann. Math. (2) **179**(3), 1121–1174 (2014)

Idempotents and Congruence $ax \equiv b \pmod{n}$

Štefan Porubský

Dedicated to the memory of Professor Wolfgang Schwarz

Abstract Alomair et al. (J Math Cryptol 4(2):121–148, 2010, Lemma 3.1) noticed the following result which seems not to appear previously explicitly in the literature: Given a nonzero $a \in \mathbb{Z}_n$, the ring of residues modulo n, such that $\gcd(a, n) = d|b$, not only there exists an element $x \in \mathbb{Z}_n$ such that $x \cdot a \equiv b \pmod{n}$, but that there even exists an invertible element $x \in \mathbb{Z}_n^*$ such that $x \cdot a \equiv b \pmod{n}$. Their sufficient and necessary condition for this says that $\gcd(b/d, n/d) = 1$ with d as above.

A typical structure result on finite commutative semigroup says that the multiplicative semigroup of $\mathbb{Z}_n$ decomposes into the so-called maximal subsemigroups belonging to the idempotents of $\mathbb{Z}_n$. Each such semigroup contains a maximal subgroup having for its identity the corresponding idempotent. In general this subgroup is a proper subset of the maximal subsemigroup containing it. However, the group of elements of $\mathbb{Z}_n$ coprime to n is an example of the case when this maximal subsemigroup and the maximal subgroup coincide (both evidently belonging to the idempotent 1).

In what follows we prove that if a congruence $x \cdot a \equiv b \pmod{n}$ is solvable there always exists a solution in the maximal semigroup belonging to the idempotent given by the divisor $\delta = \gcd(b/d, n/d)$ and if δ is a unitary divisor of n then there even exists a solution in the maximal subgroup belonging to the idempotent given by δ.

Keywords Coprime • Idempotent • Maximal group • Maximal semigroup • Solution to a congruence

Š. Porubský (✉)
Institute of Computer Science, Academy of Sciences of the Czech Republic, Pod Vodárenskou věží 2, 182 07 Praha 8-Libeň, Czech Republic
e-mail: sporubsky@hotmail.com

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_23

2010 Mathematics subject classification: Primary 11A07; Secondary 11D04, 11A05, 20M14

God does arithmetic. (‘*Ο Θεὸζ ’Αριθμητίξει.*)
C.F. Gauss

1 Starting Modifications of a Classical Result

The following result belongs to standard requisites of elementary number theory (see [6, Theorem 57] and its proof):

Lemma 1.1 *If $a, b, n \in \mathbb{Z}$, and $\gcd(a, n) = d$, then the congruence*[1]

$$ax \equiv b \pmod{n} \tag{1.1}$$

is solvable if and only if $d|b$. In the affirmative case it has just d solutions. If one solution is x_0, then the all incongruent ones are

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d} \tag{1.2}$$

Alomair et al. [1, Lemmas 3.1 and 5.5.] noticed the following surprising result which seems not to appear previously explicitly in the literature and which they applied in a construction of hash functions:

Theorem 1.2 *If $d = \gcd(a, n)$ and $d|b$, then the congruence (1.1) has a solution coprime to n if and only if $\gcd\left(\frac{b}{d}, \frac{n}{d}\right) = 1$, or equivalently if and only if $\gcd(a, n) = \gcd(b, n)$.*

The original proof of this simple result given by Alomair et al. [1] was surprisingly several pages long. A several lines proof of a slightly more general result was given in [5].[2] Here we present another proof which simplifies the original proof given by Alomair et al. [1]. Its idea will be used in the subsequent proof of a related converse question.

Proof (Proof of Theorem 1.2) Let

$$a = a_1 d, \quad b = b_1 d, \quad n = n_1 d. \tag{1.3}$$

[1] To simplify the notation and presentation all moduli and divisors will be always assumed to be positive in what follows.

[2] In [5, Theorem 2] actually the following extension was proved: (1.1) has a solution coprime to n if and only if $\gcd(a, n) = \gcd(b, n)$. If this condition is satisfied, then there are exactly $\frac{d}{\delta}\varphi(\delta)$ incongruent solutions of (1.1) coprime to n, where δ is the largest divisor of d with $\gcd(\delta, \frac{n}{d}) = 1$, and $\varphi(m)$ is the number of integers k, $1 \le k \le m$, coprime to m. For another generalization consult [10].

Then (1.1) reduces to

$$a_1 x \equiv b_1 \pmod{n_1} \quad \text{with } \gcd(a_1, n_1) = 1. \tag{1.4}$$

If $\gcd(b_1, n_1) > 1$, then the condition $\gcd(a_1, n_1) = 1$ implies that every prime p dividing $\gcd(b_1, n_1)$ necessarily divides every solution x to (1.1). To prove the sufficiency suppose that $\gcd(b_1, n_1) = 1$. Divide the primes dividing n and b, that is primes dividing $\operatorname{lcm}[d, n_1, b_1]$ into the following four groups:

- primes dividing d
  - let p denote such a prime that $p|d$ and $p \nmid n_1$, but possibly $p|b_1$,
  - let γ denote such a prime that $\gamma|d$ and $\gamma|n_1$, consequently $\gamma \nmid b_1$,
- primes not dividing d
  - let ζ denote such a prime that $\zeta|n_1$, then $\zeta \nmid b_1$ (clearly $\zeta|n$),
  - let r denote such a prime that $r|b_1$, then $r \nmid n$ (clearly $r|b$).

The modulus n can be thus divisible only by primes denoted by p, γ, or ζ. Since $\gcd(b_1, n_1) = 1$ (and $\gcd(a_1, n_1) = 1$), every solution x_0 to (1.4) is coprime to n_1. But γ's and ζ's divide n_1, and therefore x_0 cannot be divisible by some γ or ζ. Thus to find a solution coprime to n it is enough to exclude only the primes p as possible divisors.

All solutions of (1.1) are of the form

$$x_k = x_0 + kn_1 \pmod{n_1}, \quad \text{with } k = 0, 1, \ldots, d-1. \tag{1.5}$$

If no prime of the group p divides x_0 the proof is finished. In the opposite case, let $p_1, p_2, \ldots, p_s$ be those amongst the p's which divide x_0, and $p'_1, p'_2, \ldots, p'_\ell$ which do not. Take in (1.5) for k a solution, say k^*, to the system

$$n_1 k \equiv 1 \pmod{p_i}, \qquad j = 1, \ldots, s, \tag{1.6}$$

$$n_1 k \equiv 1 - x_0 \pmod{p'_j}, \qquad j = 1, \ldots, \ell. \tag{1.7}$$

Condition (1.6) assures that $p_i \nmid kn_1$ for all $i = 1, \ldots, s$, and (1.7) that $p_j \nmid x_0 + kn_1$ for $j = 1, \ldots, \ell$. Since $p_1 \cdots p_s p'_1 \cdots p'_\ell \le d$ there exists a solution k^* to (1.6) and (1.7) with $0 \le k^* \le p_1 \cdots p_s p'_1 \cdots p'_\ell - 1 < d$, and the corresponding $x_{k^*} = x_0 + k^* n_1$ fulfills the requirements of statement to be proved.

Since all solutions, if any, to (1.1) form an arithmetic progression (1.2), a reversed question can be asked with an affirmative answer:

Theorem 1.3 *Let*

$$x_0 + kN, \quad k = 0, 1, 2, \ldots, \tag{1.8}$$

be an arithmetic sequence with $\gcd(x_0, N) = 1$. *Then to every multiple* M *of* N *there exists a term of the sequence* (1.8) *such that* $\gcd(x_0 + kN, M) = 1$ *and* $k \in \{0, 1, \ldots, \frac{M}{N} - 1\}$.

A cursory argument based on Dirichlet theorem on primes in an arithmetic progression says that there is always an element (even a prime) in (1.8) which is coprime to M, but it may be very far from the beginning of the sequence. Famous Linnik's theorem says that the least prime $p(a, b)$ in the arithmetic progression $a + kb$, with $\gcd(a, b) = 1$ and $1 \le a \le b$, where k runs through the positive integers, satisfies $p(a, b) < cb^L$ with effectively computable constants c and L. It is conjectured that $p(a, b) < b^2$. Clearly, such a least prime in (1.8) is not necessarily coprime to the given M. Nevertheless, we can proof Theorem 1.3 using elementary means only.

Proof (Proof of Theorem 1.3) Divide the primes dividing $M = \frac{M}{N} \cdot N$ into four groups

1. $p|N$ and $p|\frac{M}{N}$
2. $\zeta|N$ and $\zeta \nmid \frac{M}{N}$
3. $\gamma \nmid N$ and $\gamma|\frac{M}{N}$
4. $\varrho|(x_0, M)$

Since $\gcd(x_0, N) = 1$, neither p nor ζ can divide $x_0 + kN$ for a non-negative k. Similarly $\varrho|\frac{M}{N}$.

If the set of primes γ and ϱ is empty, then $\gcd(x_0, M) = 1$. If in the opposite case one of them is non-empty and if $\gamma_1, \ldots, \gamma_s$ are all the primes of the third type, and $\varrho_1, \varrho_2, \ldots, \varrho_\ell$ all the primes of the fourth type, then any k solving the system of congruences

$$\begin{aligned} x_0 + kN &\equiv 1 \pmod{\gamma_i}, \quad i = 1, \ldots, s, \text{ if } s \ge 1 \\ kN &\equiv 1 \pmod{\varrho_j}, \quad j = 1, \ldots, \ell, \text{ if } \ell \ge 1 \end{aligned}$$

yields the required term of the given sequence.

In what follows we shall work with the ring structure of $\mathbb{Z}_n$, the ring of residue classes modulo n, where $n \in \mathbb{Z}, n \neq 0$. To work with its elements it will be sometimes more convenient to use the notation, if $x \in \mathbb{Z}$, then $[x]_n$ will denote the residue class modulo n containing x. If the modulus n will be clear from the context we shall use the abbreviation $[x]$.

As it will follow from the lines below the multiplicative semigroup $(\mathbb{Z}_n, \cdot)$ of the ring $\mathbb{Z}_n$ contains in the general case more subgroups as it is usually taken into account in the standard number theory, where the group of reduced residue classes modulo n or maximally together with the trivial subgroup $\{0\}$ are typical prototypes

of a subgroup of $(\mathbb{Z}_n, \cdot)$. Denote by $G_n(1)$ the multiplicative group of reduced residue classes modulo n.

The following elementary result, which reproves Lemma 2.1 of [11] (see also [8, Lemma 2.1][3]), will be used in what follows:

Corollary 1.4 *If $n, x \in \mathbb{Z}$, then*

$$[x]_n = [ta]_n,$$

where $t = \gcd(n, x)$ and $[a]_n \in G_n(1)$. In other words, given an $n \in \mathbb{Z}$, then for every $x \in \mathbb{Z}$ there exists an integer a coprime to n such that $x \equiv ta \pmod{n}$, where $t = \gcd(x, n)$.

Proof Write $x = tb$. Then Theorem 1.3 implies that in the progression $\frac{x}{t} + k\frac{n}{t}$ there is an a coprime to n. Clearly, $x \equiv ta \pmod{n}$.

Example 1.5 Let $n = 420$ and $x = 36$ in the ring $\mathbb{Z}$ of rational integers. Then $\gcd(420, 36) = 12$. Since $\left(\frac{36}{12}, 420\right) \neq 1$, $36 = 12.3$ is not the representation of $x = 36$ in the spirit of the Corollary. From the solutions 3, 38, 73, 108, 143, 178, 213, 248, 283, 318, 353, 388 to the congruence $3 \equiv a \pmod{35}$ incongruent mod 420 only 73, 143, 283, 353 are coprime to 420.[4]

The divisor $t = (n, x)$ of n will be called the **divisor to which** $x \in \mathbb{Z}$ **belongs** modulo n.

Our aim is to show that the result of Theorem 1.2 can be further extended. The first-stage extension is based on the fact that the subgroup $\mathbb{Z}_n^*$ of integers coprime to n—as already indicated—is not the only subgroup of the multiplicative semigroup $\mathbb{Z}_n$ of integers modulo N worth to investigate. A further immediate generalization level are the commutative principal ideal rings with identity satisfying the following finiteness condition:

(FN) *For every nonzero ideal $\mathfrak{I} \subset R$ the residue class ring $R/\mathfrak{I}$ is finite.*

This generalization can be done along the presented lines almost verbatim using the tools developed in [8]. A generalization to more general classes of commutative ring will be a subject of a forthcoming paper.

[3] In [11] Š. Schwarz deals only with integers. In [8] the theory developed in [11] is extended and generalized to a wider class of commutative rings. The author of [11], as one of founders of the semigroup theory (cf. [7] or [2, 3]), tried to minimalize the usage of the addition operation in the proofs, while in [8] we based the reasoning on an unrestricted usage of the ring structure of the set of integers and its generalizations. This approach led to another symbolics of which simplified version will be used in this paper. For an overview of results proved by the idempotents approach cf. [9].

[4] This simple example also shows that the need to find coprime solutions of congruences, which existence is proved in Theorem 1.2, is not unusual, but nobody formulated this explicitly prior to [1].

2 Idempotents and Group Elements

We shall use the terminology introduced in [8]. For reader's convenience we shall repeat some basic facts in this section.

If $n \in \mathbb{Z}$, then the **cyclic** or **monogenic semigroup** $s(x,n)=\{[x]_n,\ [x]_n^2,\ [x]_n^3,\ \dots\}$ **generated by an** $x \in \mathbb{Z}$ is finite and therefore there exist the least positive integers $k = k(x,n)$, and $d = d(x,n)$ such that $x^t \equiv x^{t+d} \pmod{n}$ for all $t \geq k(x,n)$, $t \in \mathbb{Z}$. The integer k is called the **index** of x, and d is called the **period** of x modulo n. Consequently the cyclic semigroups generated by x have the form

$$[x]_n, [x]_n^2, \dots, [x]_n^{k-1}, [x]_n^k, \dots, [x]_n^{k+d-1}, [x]_n^k, \dots. \tag{2.1}$$

The previous result was epitomized by Schwarz [11] as the individual Fermat–Euler theorem (cf. also [8, Theorem 1.9]):

Lemma 2.1 *If $x \in \mathbb{Z}$, then*

$$x^{k(x)+d(x)} \equiv x^{k(x)} \pmod{n}$$

and the numbers $k(x)$ and $d(x)$ are the least positive numbers with this property.

An older theorem of Frobenius (cf. [8, Theorem 1.1]) says that the periodically repeating set $\{[x]_n^k, \dots, [x]_n^{k+d-1}\}$ in (2.1) forms a cyclic group with respect to the multiplication in $\mathbb{Z}_n$. Its identity element, say $[e]_n$, is an idempotent in $\mathbb{Z}_n$, i.e., $e \equiv e^2 \pmod{n}$. Moreover, the element $[e]$ is the unique idempotent of $\mathbb{Z}_n$ which belongs to $s(x,n)$ what is usually phrased that **the element** x **belongs to the idempotent** e. The idempotent to which $a \in \mathbb{Z}$ belongs modulo n will be denoted by $i(a,n)$, or simply $i(a)$ if the modulus n is clear from the context.

The set

$$P_n(e) = \{x \in R\ ;\ x \text{ belongs to } e\}$$

is the largest subsemigroup of $(\mathbb{Z}_n, \cdot)$, which except for e contains no other idempotent of $\mathbb{Z}_n$ (see [8, Theorem 1.2]). By this property uniquely determined maximal subsemigroup $P_n(e)$ of $(\mathbb{Z}_n, \cdot)$ containing e will be called the **maximal (multiplicative) semigroup belonging to the idempotent** e.

It follows easily that $\mathbb{Z}_n = \bigcup_{e \in E} P_n(e)$ where $E = E_n$ denotes the set of all idempotents in $\mathbb{Z}_n$, and that the union is disjoint.

If $[e] \in E_n$ is an idempotent, then there always exists a subgroup of $(\mathbb{Z}_n, .)$ containing $[e]$ as its identity, e.g., the group $\{[e]\}$, or the subgroups of any cyclic semigroups $s(x,n)$ with $[e]_n$ as the identity in the above-mentioned Frobenius result. It can be shown that there always exists a (unique) maximal subgroups of $(\mathbb{Z}_n, \cdot)$ amongst all the subgroups of $\mathbb{Z}_n$ which identity element is the given idempotent $[e] \in E_n$. This group $G_n(e)$ is called the **maximal (multiplicative) subgroup of** $(\mathbb{Z}_n, .)$ **belonging to the idempotent** $e \in E_n$ (see [4] or [8]). Since $G_n(e) \subset P_n(e)$

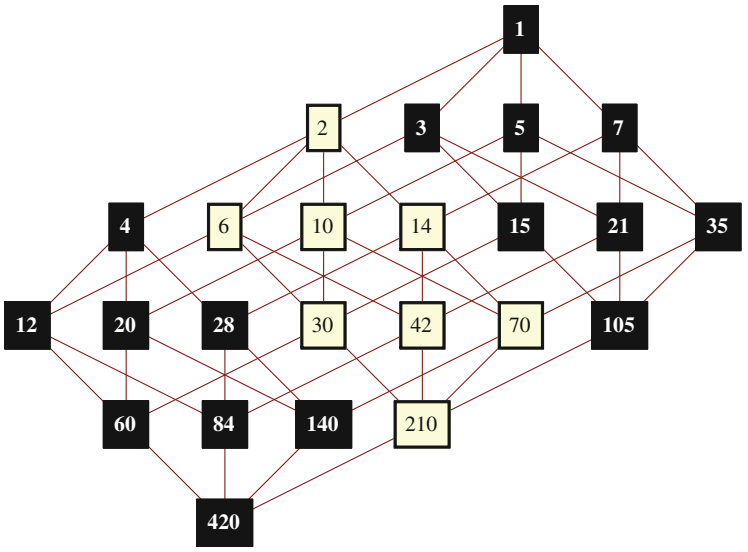


Fig. 1 Hasse diagram of the divisibility structure of all divisors of $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ (unitary divisors are represented with *black background*)

two such maximal groups are either disjoint or identical. Generally, if $[a] \in \mathbb{Z}_n$ belongs to a multiplicative subgroup of $\mathbb{Z}_n$ we say that $[a]$ or a is a **group member** modulo n.

Note that always[5] $G_n(1) = P_n(1)$, but $P_n(0)$ as the set of nilpotent elements of $\mathbb{Z}_n$ is usually a proper overset of $G_n(0) = \{0\}$.

The set E_n can be endowed with an (partial) order[6]

$$x \leq y \quad \Longleftrightarrow \quad xy = x.$$

We immediately have

Lemma 2.2 *We have* $i(a, n) \geq i(ab, n)$ *for every* $a, b, n \in \mathbb{Z}$.

Let t be a divisor of n. We say that t is a **unitary divisor**[7] of n if $\gcd(t, \frac{n}{t}) = 1$. The unitary divisor d of an n will be said to be **generated by** t if both t and d have the same set of prime divisors. The unitary divisor d of n generated by a $t|n$ will be denoted by $u(t, n)$, or simply $u(t)$.

[5] cf. Lemma 2.6.

[6] For instance, an idempotent $e \in E_n$ is called **primitive** if it is minimal in the ordered set $(E_n \setminus \{0\}, \leq)$, and **maximal** if it is maximal in $(E_n \setminus \{1\}, \leq)$, but we shall not use these notions, even if they play an important role in [8].

[7] Note that if $n = \pm 1 p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}$ then the number of unitary divisors of n is 2^r and every of them is of the form $\prod_{j \in J} p_j^{u_j}$ for some $J \subset \{1, 2, \ldots, r\}$. For example, see Fig. 1.

Note that if $e, f \in E_n$ are two idempotents of $\mathbb{Z}_n$, then the relation $e \le f$ can be equivalently expressed in the form $u(f,n)|u(e,n)$.

Lemma 2.3 ([8, Theorem 2.1]) *There exists a one-to-one correspondence between unitary divisors of n and idempotents of the residue class ring $\mathbb{Z}_n$. More precisely, every idempotent of $\mathbb{Z}_n$ is expressible in the form $[ta]$, where t is a unitary divisor of n and $[a] \in G_n(1)$ is given by a solution to the congruence*

$$ta \equiv 1 \pmod{\frac{n}{t}}. \tag{2.2}$$

If $f \in E_n$ and $[f]_n = [ta]_n$, $[a] \in G_n([1])$, then we say that $[f]_n$ is the **idempotent belonging to the (unitary) divisor** t (of n, if the modulus is not clear from the context). Denote this idempotent by $i(t,n)$, or more precisely $i(u(d,n),n)$ where $d|n$. Note that Theorem 2.3 and the following Lemma 2.4 guarantee that there is no ambiguity with the previously introduced symbol $i(a,n)$ assigned to an element $a \in R$. In a similar way we can write $u(a,n)$ for the unitary divisor of n generated by the $\gcd(a,n)$.

Lemma 2.4 *Let $x, n \in \mathbb{Z}$ and $t = \gcd(n,x)$. If $u(t,n)$ is the unitary divisor to which the idempotent $i(x,n)$ belongs, then we have $u(\gcd(x,n),n) = u(\gcd(i(x,n),n),n)$.*

Proof Let $[x] = [ta]$ and $[i(x,n)] = [db]$ with $a, b \in G_n(1)$, be representations of x and $i(x,n)$ given by Corollary 1.4. Since $[x]^k = [i(x,n)]$ for some k, the divisors t, d of n must have the same set of prime divisors, and the Lemma follows.

There follows from [8, Theorem 2.4] that:

Lemma 2.5 *Let $[f] \in \mathbb{Z}_n$ be the idempotent belonging to the unitary divisor d of n. Then*

$$G_n(f) = [d]G_n(1) \tag{2.3}$$

and

$$P_n(f) = G_n(f) \cup \bigcup_{\substack{t|d, t<d \\ u(t,n)=d}} [t]G_n(1). \tag{2.4}$$

Another important interrelation between $P_n(e)$ and $G_n(e)$, $e \in E_n$ is shown in the following result:

Lemma 2.6 ([8, Corollary 1 of Theorem 1.3]) *If $e \in E_n$, then*

$$G_n(e) = P_n(e)e, \tag{2.5}$$

specifically for $e = 1$ we have $G_n(1) = P_n(1)$.

Moreover

Lemma 2.7 *If $e, f \in E_n$, then*

$$G_n(e)f = G_n(ef) \tag{2.6}$$

and consequently for $e = 1$

$$G_n(1)f = G_n(f). \tag{2.7}$$

Suppose that

$$n = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}, \tag{2.8}$$

is the standard form of a modulus n, $n \in \mathbb{Z}$.

The next results show how it can be determined which power of an element $[x] \in \mathbb{Z}_n$ belongs to a (maximal) subgroup of $\mathbb{Z}_n$.

Let $[x] \in \mathbb{Z}_n$ be an element belonging to the divisor $d = \prod_{j=1}^{r} p_j^{v_j}$, where $0 \leq v_j \leq u_j$. Then define (see [8, Theorem 2.5] or [4])

$$\nu([x]) = \begin{cases} 1, & \text{if } d = 1, \\ \max\limits_{\substack{j \in \{1,\ldots,r\} \\ v_j \neq 0}} \left\lceil \frac{u_j}{v_j} \right\rceil, & \text{otherwise.} \end{cases} \tag{2.9}$$

Lemma 2.8 ([8, Theorem 2.5]) *For every $x \in \mathbb{Z}$ we have $k(x, n) = \nu([x])$. Consequently, $[x]^t$ is a group element of $(\mathbb{Z}_n, \cdot)$ if and only if $t \geq \nu([x])$.*

Corollary 2.9 *If n is square-free,*[8] *then $P_n(e) = G_n(e)$ for every idempotent e of $\mathbb{Z}_n$.*

For further relationships between maximal semigroups and maximal groups in $\mathbb{Z}_n$ consult [8].

3 Idempotents and the Solvability of $ax \equiv b \pmod{n}$

In this part we prove some results about the solvability of congruence (1.1) in terms of idempotents to which parameters a, b, and n of this congruence belong.

Theorem 3.1 *If the congruence (1.1) has a solution x_0, then $i(a, n) \cdot i(x_0, n) = i(b, n)$. Consequently $i(a, n) \geq i(b, n)$, and $i(x_0, n) \geq i(b, n)$.*

[8] That is, $u_1 = \cdots = u_r = 1$ in (2.8).

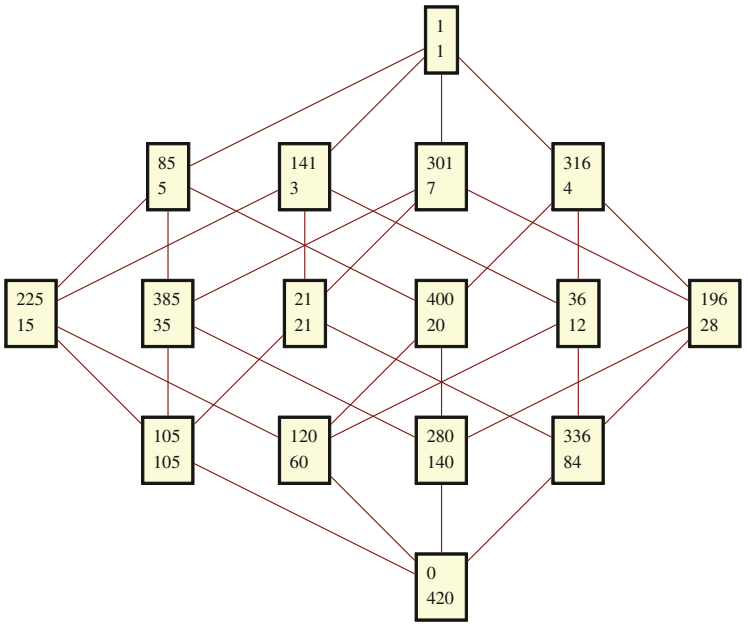


Fig. 2 Hasse diagram of the divisibility structure of idempotents in $\mathbb{Z}_{420}$ (the idempotent is in the first row, its unitary divisor in the second one)

Proof If there is an x_0 such that $ax_0 = b \pmod n$, let $i(a) = a^k$, $i(x_0) = x_0^\ell$, $i(b) = b^n$. If $K = \operatorname{lcm}\{k, \ell, n\}$, then $a^K x_0^K = b^K$, which implies $i(a)i(x_0) = i(b)$. Consequently

$$i(a) \cdot i(b) = i(a) \cdot (i(a) \cdot i(x_0)) = (i(a) \cdot i(a)) \cdot i(x_0) = i(a) \cdot i(x_0) = i(b)$$

and

$$i(b) \cdot i(x_0) = (i(a) \cdot i(x_0)) \cdot i(x_0) = i(a) \cdot i(x_0) = i(b),$$

and the Lemma follows.

Unfortunately, the condition $i(a) \geq i(b)$ of Theorem 3.1 is not sufficient for a solvability of congruence (1.1) in general:

Example 3.2 Consider the congruence $4x \equiv 6 \pmod{420}$. Since $\gcd(4, 420) = 4$, the congruence is not solvable. On the other hand, in the ring $\mathbb{Z}_{420}$ we have $i(6) = 36$, $i(4) = 316$, and $[36] \leq [316]$ (see Fig. 2).

In the previous Example 3.2 we have $[6] \in P_{420}(36) \setminus G_{420}(36)$ (and $[4] \in G_{420}(316)$), i.e., $[6]$ is not a group element. In the opposite case we have

Theorem 3.3 *If $i(a,n) \geq i(b,n)$ and $[b]_n$ is a group element,*[9] *then the congruence (1.1) is solvable in $\mathbb{Z}$.*

Proof If $i(a) \geq i(b)$, then $i(a) \cdot i(b) = i(b)$. First we prove that[10]

$$P_n(i(a)) \cdot i(b) \subset G_n(i(b)).$$

If $[x] \in P_n(i(a))$, then $[x]^t = i(a)$ for some positive integer t. Consequently, $([x] \cdot i(b))^t = i(a) \cdot i(b) = i(b) \in G_n(i(b))$. Moreover (Lemma 2.7) $G_n(i(b)) = G_n(1)i(b)$. Thus there exists a $y \in G_n(1)$ such that $[a] \cdot i(b) = [y] \cdot i(b)$. Then $i(b) = [a] \cdot [y]^{-1} \cdot i(b)$. Since $b \in G_n(i(b))$ due to our assumption and $G_n(i(b)) = P_n(i(b)) \cdot i(b)$ due to Lemma 2.6, there exits a $t \in P_n(i(b))$ with $i(b) \cdot t = [b]$. Then $x = a \cdot y^{-1} \cdot i(b) \cdot t$ solves (1.1).

Example 3.4 A sufficient condition for $[b] \in G_n(i(b))$ is the equality $G_n(i(b)) = P_n(i(b))$.[11] If $n = 420$ we have $G_{420}(e) = P_{420}(e)$ for the following idempotents:

$$e \in \{1, 21, 85, 105, 141, 225, 301, 385\}.$$

Here $[120]_{420} \leq [400]_{420}$ (cf. Fig. 2), $P_{420}(400) = \{10, 20, 40, 50, 80, 100, 110, 130, 160, 170, 190, 200, 220, 230, 250, 260, 290, 310, 320, 340, 370, 380, 400, 410\}$, $P_{420}(120) = \{30, 60, 90, 120, 150, 180, 240, 270, 300, 330, 360, 390\}$ and $G_{420}(120) = \{60, 120, 180, 240, 300, 360\}$. Clearly, all $24 \cdot 6 = 144$ possible combinations $[a] \in P_{420}(400)$ and $[b] \in G_{420}(120)$ lead to a solvable congruence $ax \equiv b \pmod{420}$.

On the other hand, neither the condition $G_n(i(b)) = P_n(i(b))$ nor $[b] \in G_n(i(b))$ is necessary for the solvability of congruence (1.1).

Example 3.5 In congruence $6x \equiv 42 \pmod{420}$ we have $i(6) = [36] \geq i(42) = [336]$ and $P_{420}(336) = \{42, 84, 126, 168, 252, 294, 336, 378\} \supsetneq G_{420}(336) = \{84, 168, 252, 336\}$. Nevertheless, the congruence is solvable.[12]

Another additional condition completing the first condition of Theorem 3.1 and securing the solvability of (1.1) says

Theorem 3.6 *Let $a, b, n \in \mathbb{Z}$. If $\gcd(b, n)$ is a unitary divisor of n, then the condition $i(a,n) \geq i(b,n)$ is also sufficient for the solvability of the congruence (1.1).*

Proof In $\mathbb{Z}_n$ condition $i(a) \geq i(b)$ means that

$$\operatorname{lcm}(u(b,n), u(a,n)) = u(b,n).$$

[9] That is, $[b] \in G_n(i(b))$.

[10] Note that Lemma 2.6 shows that $P_n(i(b)) \cdot i(b) = G_n(i(b))$.

[11] This condition is satisfied for every idempotent if n is square-free as it follows from Corollary 2.9.

[12] Having, by the way, the same set of solutions as the congruence in Example 3.8.

In other words, every prime divisor of a dividing n also divides b. Since $u(b,n)$ is a unitary divisor of n, every prime power dividing $\gcd(a,n)$ divides also b, that is $\gcd(a,n)|b$, what is the necessary and sufficient condition for solvability of congruence (1.1).

Lemma 2.5 implies that every element of $G_n(i(b))$ is divisible by the unitary divisor $u(b,n)$ and (2.4) shows that these are the only elements in $P_n(i(b))$ (and consequently in the whole $\mathbb{Z}_n$) possessing this property. Thus Theorem 3.6 is also a consequence to Theorem 3.3.

Theorem 3.7 *If x_0 is a solution to (1.1), $d = \gcd(a,n)$ and $\delta = \gcd\left(\frac{b}{d}, \frac{n}{d}\right)$, then*

$$i(b,n) \le i(x_0,n) \le i(\delta,n). \tag{3.1}$$

Proof The left-hand side inequality follows from Theorem 3.1. To prove the right-hand side, let, as in proof of Theorem 1.2, write $a = a_1 d$, $b = b_1 d$, and $n = n_1 d$. Then (1.1) reduces to (1.4). If a prime p divides $\delta = \gcd(b_1, n_1)$, then $p|n_1$ and $p \nmid a_1$. Consequently, $p|x_0$ and thus every prime dividing $u(\delta,n)$ also divides $u(x_0,n)$, that is $u(\delta,n)|u(x_0,n)$, or $i(x_0,n) \le i(\delta,n)$.

Example 3.8 Consider the congruence

$$18x \equiv 126 \pmod{420}. \tag{3.2}$$

Here $\gcd(18,420) = 6 = 2 \cdot 3$, $\gcd(126,420) = 42 = 2 \cdot 3 \cdot 7$, $i(18,420) = [36]$, $i(126,420) = [336]$, $[18] \in P_{420}(36) \setminus G_{420}(36)$, and $[126] \in P_{420}(336) \setminus G_{420}(336)$. Further $\delta = \gcd\left(\frac{126}{6}, \frac{420}{6}\right) = \gcd(21,70) = 7$, $i(7,420) = [301]$.

The set of all incongruent solutions mod 420 is

$$7, 77, 147, 217, 287, 357.$$

They belong to the following idempotents mod 420

$$21, 301.$$

The distribution of solutions in groups and semigroups belonging to corresponding idempotents is tabbed in Table 1.

Example 3.8 also shows that a fulfillment of the chain of inequalities (3.1) is not sufficient for an x_0 to be a solution. In this example $\delta = 7$, $i(7,420) = [301]$

Table 1 Distribution of solutions to $6x \equiv 42 \pmod{420}$

e	$G_{420}(e)$	$P_{420}(e)$
[21]	147, 357	Ø
[301]	7, 77, 217, 287	Ø

and $i(42, 336) = [336]$. However, there is no solution belonging to the idempotent $[196] = i(28, 420)$ lying between $[301]$ and $[336]$.

The following result gives our first possible generalization of Theorem 1.2:

Theorem 3.9 *Let $d = \gcd(a, n)$ and $d|b$. Let $\delta = \gcd\left(\frac{b}{d}, \frac{n}{d}\right)$. Then a congruence (1.1) has a solution x_0 belonging to $P_n(i(\delta, n))$.*

Proof Suppose that besides (1.3) we also have

$$b_1 = \delta b_2, \quad n_1 = \delta n_2. \tag{3.3}$$

Then given a solution x_0 to (1.1) we can also write $x_0 = \delta x_2$ and (1.1) reduces to

$$a_1 x_2 \equiv b_2 \pmod{n_2}. \tag{3.4}$$

Since $\gcd(b_2, n_2) = 1$, all solutions to congruence (3.4) are of the form $x_2' + kn_2$ with a suitable x_2' satisfying $\gcd(x_2', n_2) = 1$. Then $a_1 \cdot (\delta x_2') \equiv \delta b_2 \pmod{\delta n_2}$, and also $a_1 d \cdot (\delta x_2') \equiv db_1 \pmod{dn_1}$. In other words, $\delta x_2'$ solves the original congruence (1.1).

Theorem 1.3 implies that there is an $x'' \equiv x_2' \pmod{n_2}$ such that $\gcd(x'', n_1) = 1$. Thus $\delta x''$ solves (1.1) and simultaneously $\delta x'' \in P_n(i(\delta, n))$ according to Corollary 1.4 and Lemma 2.5.

Note that Example 3.8 shows that a congruence (1.1) satisfying conditions of Theorem 3.9 can have further solutions not belonging to $P_n(i(\delta, n))$.

In the case of coprime solutions handled in Theorem 1.2 we have $\delta = 1$. In this case we have $G_n(1) = P_n(1)$ for every n, that is every solution to (1.1) which is coprime to its modulus n is immediately a group element. However in the case of a general idempotent $e \in E_n$ we have, as already noticed several times, $G_n(e) \subsetneq P_n(e)$. Therefore not every solution to (1.1) belonging to $P_n(i(\delta, n))$ must be a group element. Nevertheless, our previous results imply the following second and possibly more close generalization of Theorem 1.2:

Corollary 3.10 *Let $d = \gcd(a, n)$ and $d|b$. Let $\delta = \gcd\left(\frac{b}{d}, \frac{n}{d}\right)$. Then a congruence (1.1) has a solution x_0 which is a group element[13] if and only if δ is a unitary divisor of n.*

Proof If δ is a unitary divisor of n, then every solution to (1.1) is divisible by δ and Theorem 2.5 finishes the proof.

Note that if n is square-free then Corollary 2.9 implies that $G_n(e) = P_n(e)$ for every idempotent $e \in \mathbb{Z}_n$, and consequently:

Corollary 3.11 *Let n be square-free and $\gcd(a, n)|b$. Then every solution to a congruence (1.1) is a group element.*

Example 3.12 Let $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$. The Hasse diagrams of its divisors and idempotents in $\mathbb{Z}_{210}$ are given in Fig. 3.

[13] More precisely belonging to the group $G_n(i(\delta, n))$.

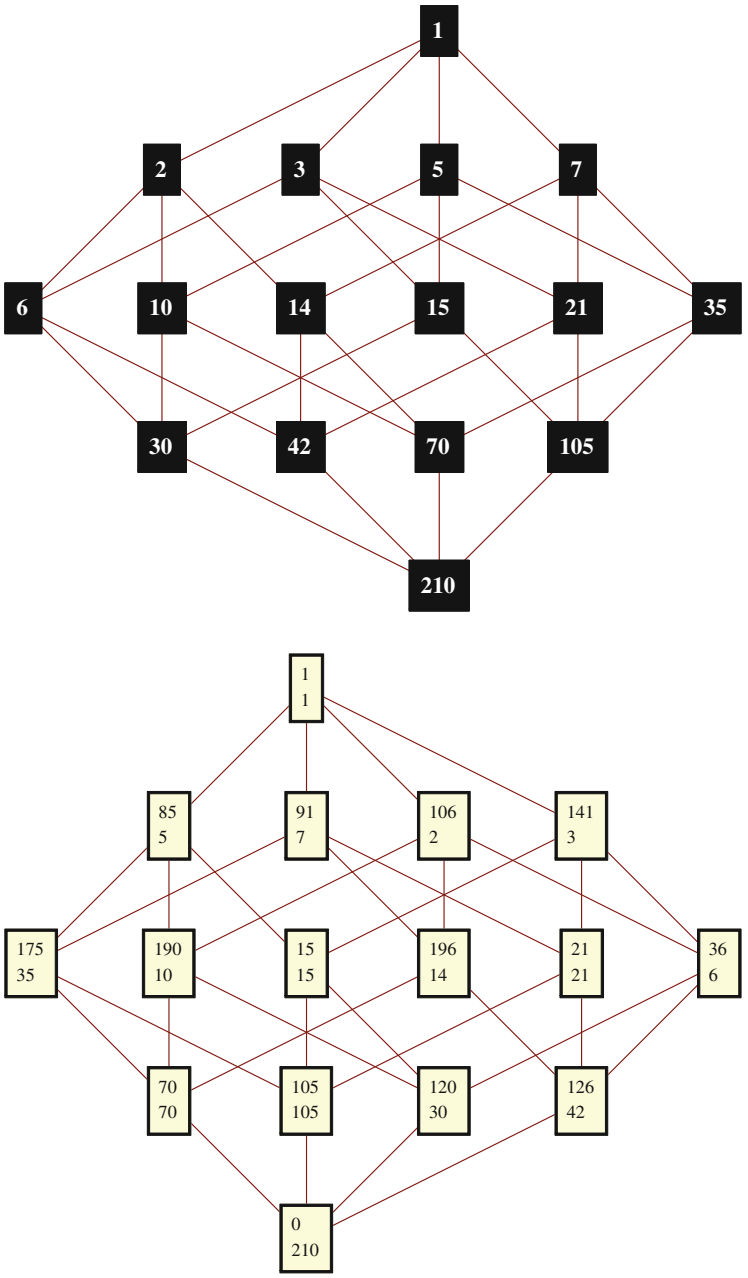


Fig. 3 Hasse diagrams of the divisors (*top*) and the idempotents in case of modulus $n = 210$

Consider the congruence

$$18x \equiv 84 \pmod{210}. \tag{3.5}$$

Here $\gcd(18, 210) = 6 = 2 \cdot 3$, $\gcd(84, 210) = 42 = 2 \cdot 3 \cdot 7$, $i(18, 210) = [36]$, $i(184, 210) = [126]$, $[18] \in P_{210}(36) = G_{210}(36)$, and $[126] \in P_{210}(336) = G_{210}(336)$. Further $\delta = \gcd\left(\frac{84}{6}, \frac{210}{6}\right) = \gcd(14, 35) = 7$, $i(7, 210) = [91]$.

The set of all incongruent solutions mod 210 is

$$28, 63, 98, 133, 168, 203.$$

They belong to the following idempotents mod 420

$$21, 91, 126, 196.$$

The distribution of solutions in groups and semigroups belonging to corresponding idempotents is tabbed in Table 2.

It is easy to find a solvable congruence (1.1) with no solution coprime to n. Example 3.8 shows that it is possible that a congruence (1.1) has no solution coprime to its modules, but has solutions being group elements. The following example shows a case of a congruence (1.1) having only solutions being group elements including coprime ones and of type not covered by Corollary 3.11:

Example 3.13 Consider the congruence

$$231x \equiv 63 \pmod{420}. \tag{3.6}$$

Here $231 = 3 \cdot 7 \cdot 11$, $63 = 3^2 \cdot 7$, $\gcd(231, 420) = \gcd(63, 420) = 21 = 3 \cdot 7$, and $i(231, 420) = i(63, 420) = [21]$ and $\{[63], [231]\} \in G_{420}(21) = P_{420}(21)$. Further $\delta = \gcd\left(\frac{63}{21}, \frac{420}{21}\right) = \gcd(3, 20) = 1$, i.e., $i(1, 420) = [1]$.

The set of all incongruent solutions mod 420 is

$$13, 33, 53, 73, 93, 113, 133, 153, 173, 193, 213, 233, 253, 273, 293, \ 313, 333, 353, 373, 393, 413.$$

They belong to the following idempotents mod 420

$$1, 21, 141, 301.$$

Table 2 Distribution of solutions to $18x \equiv 84 \pmod{210}$

e	$G_{420}(e) = P_{420}(e)$
[21]	63
[91]	133, 203
[126]	168
[196]	28, 98

Table 3 Distribution of solutions to $231x \equiv 63 \pmod{420}$

e	$G_{420}(e)$	$P_{420}(e)$
[1]	13, 53, 73, 113, 173, 193, 233, 253, 293, 313, 353, 373	$\emptyset$
[21]	273	$\emptyset$
[141]	33, 93, 153, 213, 333, 393	$\emptyset$
[301]	133, 413	$\emptyset$

Table 4 Distribution of solutions to $231x \equiv 42 \pmod{420}$

e	$G_{420}(e)$	$P_{420}(e)$
[36]	$\emptyset$	102, 162, 222, 282, 342, 402
[196]	$\emptyset$	182, 322
[316]	$\emptyset$	2, 22, 62, 82, 122, 142, 202, 242, 262, 302, 362, 382
[336]	$\emptyset$	42

The distribution of solutions in groups and semigroups belonging to corresponding idempotents is tabbed in Table 3.

The following example shows that there are congruences with no solution being a group element at all:

Example 3.14 Consider the congruence

$$231x \equiv 42 \pmod{420}. \tag{3.7}$$

Here $231 = 3 \cdot 7 \cdot 11$, $42 = 2 \cdot 3 \cdot 7$, $\gcd(231, 420) = 21$, $\gcd(42, 420) = 42$, and $i(231, 420) = [21]$, $i(42, 420) = [336]$ while $[231] \in G_{420}(21) = P_{420}(21)$, $[42] \in P_{420}(336) \setminus G_{420}(336)$. Further $\delta = \gcd\left(\frac{42}{21}, \frac{420}{21}\right) = \gcd(2, 20) = 2$, $i(2, 420) = [316]$.

The set of all incongruent solutions mod 420 is

$$2, 22, 42, 62, 82, 102, 122, 142, 162, 182, 202, 222, 242, 262, 282, 302, 322, 342, 362, 382, 402.$$

They belong to the following idempotents mod 420

$$36, 196, 316, 336.$$

The distribution of solutions in groups and semigroups belonging to corresponding idempotents is tabbed in Table 4.

The final example shows that it possible to have both group element solutions and non-group element solutions:

Example 3.15 Consider the congruence

$$6x \equiv 36 \pmod{420}. \tag{3.8}$$

Table 5 Distribution of solutions to $6x \equiv 36 \pmod{420}$

e	$G_{420}(e)$	$P_{420}(e)$
[36]	216	6
[316]	76,356	146,286

Here $6 = 2 \cdot 3$, $36 = 2^2 \cdot 3^2$, $\gcd(6, 420) = 6$, $\gcd(36, 420) = 12 = 2^2 \cdot 3$, and $i(6, 420) = i(36, 420) = [36]$, and clearly $[36] \in G_{420}(36)$. Further $\delta = \gcd\left(\frac{36}{6}, \frac{420}{6}\right) = \gcd(6, 70) = 2$, $i(2, 420) = [316]$.

The set of all incongruent solutions mod 420 is

$$6, 76, 146, 216, 286, 356.$$

They belong to the following idempotents mod 420

$$36, 316.$$

The distribution of solutions in groups and semigroups belonging to corresponding idempotents is tabbed in Table 5.

4 Wolfgang Schwarz, Me, and the Role of Idempotents

The mathematical content of this paper is actually a collection of corollaries to a part of work done during my stay at the J.W.Goethe Universität in Frankfurt am Main as a fellow of the Alexander von Humboldt (AvH) Foundation in 1980/81. The part of my research devoted to properties of idempotents later served as the basis of my joint paper [8] with my Ph.D. student and collaborator M.Laššák. I had spent 12 months in Frankfurt starting in October 1980 under supervision of Professor Wolfgang Schwarz. I have a vivid memory of the excellent mathematical library on Robert–Mayer–Strasse to which I was given access immediately after my arrival at the railway station in Frankfurt. I received the library key even earlier than the key to the flat in Beethovenstrasse where I lived for the duration of my stay. Getting a key to the library was a big surprise to me because at that time it was impossible for me and my coworkers to enter my home institute library in the absence of the librarian, and here it was a common thing even also for me from an "enemy country" (which was an official political jargon for countries behind the Iron Curtain). I spent a lot of time and many weekends in this library. Motivated by the paper [11], I conducted a systematic literature research in this library on the history of the idempotents and their role in the ring theory, including the crucial paper [4] on the group elements.

This significantly expanded my previous knowledge on the role of idempotents in the semigroup theory advocated by Professor Štefan Schwarz[14] in his paper [11].

I met Prof. Wolfgang Schwarz for the first time during a number theory conference in Debrecen (Hungary) in 1974. Later he encouraged me to apply for the above-mentioned fellowship from the AvH Foundation. My stay in Frankfurt gave me an impetus and motivation for various non-mathematical activities. For instance, after my return I convinced the other Schwarz, Professor Štefan Schwarz, to allow us to visit the library in my institute also at a time when no librarian was present.

One of the activities of Professor Wolfgang Schwarz which I admired greatly was his service as a "Vertrauensdozent der Frankfurter Hochschulgruppe" of the Cusanuswerk,[15] a position he was very proud of. As a part of this service he invited two to three dozen students of various specializations to his home in Ruppertshain twice a year. There he organized an evening party that included a colloquial lecture on a topic of general interest for these students. These evenings were one of the most pleasant experiences that left an indelible imprint on my stay in Frankfurt. Last but not least, it was Professor W. Schwarz and his wife Doris who invited me and my whole family to visit them immediately after the collapse of the communism in Czechoslovakia. It was our first joint family visit to a western country. Previously I was able to travel with my wife only under the condition that our children stayed at home. Later we had visited them on number of occasions. To this day, all of my family treasure the hospitality we had enjoyed. *Lieber Herr Schwarz, Ehre Ihrem Andenken*!

Acknowledgements The author "Štefan Porubský" was supported by the Grant Agency of the Czech Republic, Grant # P201/12/2351 and the strategic development financing RVO 67985807. All computations and figures were done using *Mathematica* program package.

References

1. B. Alomair, A. Clark, R. Poovendran, The power of primes: security of authentication based on a universal hash-function family, J. Math. Cryptol. **4**(2), 121–148 (2010)
2. A.H. Clifford, G.B. Preston, *The Algebraic Theory of Semigroups*. Mathematical Surveys 7, vol. I (American Mathematical Society, Providence, 1961)

[14]It is necessary to mention here that in my professional life two Schwarzs had played a significant motivating role. Beside Wolfgang Schwarz, this second one—Štefan Schwarz—had been the director of my home institute at the Slovak Academy of Sciences in Bratislava for two decades. I owe him my gratitude for creating favorable working conditions there. Also, without his help I would have never obtained a permission from local authorities to apply for an AvH Foundation scholarship.

[15]The Cusanuswerk is the scholarship body of the Catholic Church in Germany and awards government scholarships to exceptionally gifted Catholic students in all branches of academic study.

3. A.H. Clifford, G.B. Preston, *The Algebraic Theory of Semigroups*. Mathematical Surveys 7, vol. II (American Mathematical Society, Providence, 1967)
4. H.K. Farahat, L. Mirsky, Group membership in rings of various types, Math. Z. **70**, 231–244 (1958)
5. O. Grošek, Š. Porubský, Coprime solutions to $ax \equiv b \pmod{n}$, J. Math. Cryptol. **7**, 217–224 (2013)
6. G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, 5th edn. (Oxford at the Clarendon Press, Oxford, 1979)
7. Ch. Hollings, *Mathematics Across the Iron Curtain. A History of the Algebraic Theory of Semigroups*. History of Mathematics, vol. 41 (American Mathematical Society, Providence, 2014)
8. M. Laššák, Š. Porubský, Fermat-Euler theorem in algebraic number fields. J. Number Theory **60**(2), 254–290 (1996)
9. Š. Porubský, Idempotents, Group Membership and Their Applications. Math. Slovaca (submitted)
10. Š. Porubský, New solvability conditions for congruence ax ≡ b (mod n). Tatra Mt. Math. Publ. **64**, 93–99 (2015)
11. Š. Schwarz, The role of semigroups in the elementary theory of numbers, Math. Slovaca **31**(4), 369–395 (1981)

Recent Developments on the Edge Between Number Theory and Graph Theory

Jürgen Sander and Torsten Sander

Dedicated to the memory of Wolfgang Schwarz[1]

Abstract This article reflects some of the authors' perspectives on and personal experiences with the interplay between number theory and graph theory. To start with, we touch on a few historical milestones of the rewarding relations between the two disciplines. Later on, we shall address more recent developments without any ambition to strive for completeness.

Keywords Cayley graph • Circulant graph • Graph energy • Graph spectrum • Integral graph • Multiplicative function • Primes in graphs • Ramanujan graph

2010 Mathematics subject classification: Primary 05C50, 11A25, 11L03; Secondary 15A18

[1]Who appreciated the use of footnotes. As a tribute to him, we pursue his habit with great pleasure.

The first author met Wolfgang Schwarz for the first time at the DMV-Tagung (Meeting of the Deutsche Mathematiker-Vereinigung) in 1986 in Marburg, and from then on again and again at various conferences. Schwarz's quiet and reflected, but also determined appearance left a lasting impression. One of the valuable memories still is the daily joint 'hiking exercise' after lunch up to the 8th floor of the maths building, when the first author had accepted Schwarz's invitation as guest professor at Frankfurt University.

J. Sander (✉)
Institut für Mathematik und Angewandte Informatik, Universität Hildesheim,
31141 Hildesheim, Germany
e-mail: sander@imai.uni-hildesheim.de

T. Sander
Fakultät für Informatik, Ostfalia Hochschule für angewandte Wissenschaften,
38302 Wolfenbüttel, Germany
e-mail: t.sander@ostfalia.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_24

1 Introduction and Some Highlights in History

Besides geometry, number theory is considered to be one of the founding fields of their science by almost all mathematicians.[2] As against number theory, graph theory — at least considered as a mathematical discipline — is undoubtedly young. Although many textbooks emphasize Euler's solution to the famous problem of the seven bridges of Königsberg[3] from 1736 to be the first graph-theoretical paper, graphs as a mathematical concept did not make an explicit appearance in it.[4] In fact, Euler himself denied to consider his proof as an application of 'true' mathematics.

As usual it took quite some time before the formal mathematical notion of a graph was established. It was Sylvester who introduced the term *graph* in 1878 in the context of chemistry.[5] The birth of graph theory as a scientific discipline in its own right was marked by the treatize *Die Theorie der regulären graphs*[6] published by Petersen in 1891. In the years that followed the new field grew rapidly. The first and for many years only textbook on graph theory[7] was published by Denés Kőnig in 1936. A lot of fundamental results originated from the 1930s.

Even at this early stage the first interrelations between number theory and graph theory occurred. An important example is what is now called *Ramsey theory*, dealing with the following question:

> Assume that a set S has a certain property. Under which assumptions are we able to guarantee that, after partitioning S, at least one of the subsets of S still has that property?

If it holds, this concept may be viewed as a generalization of the *box principle* (or *pidgeon hole principle*): *after partitioning a set S with $|S| \geq 2$ into less than $|S|$ subsets, there is at least one subset with again ≥ 2 elements.* In 1930 Ramsey published an article formulated in terms of formal logic.[8] Nowadays the classical results of Ramsey are usually formulated in the language of graph theory.

[2] For a very readable discussion on the formation of number theory as a discipline we recommend the essay *A book in search of a discipline* by C. Goldstein and N. Schappacher in: *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, C. Goldstein, N. Schappacher, J. Schwermer (eds.), Springer, 2007.

[3] L. Euler, *Solutio problematis ad geometriam situs pertinentis*, Commentarii Academiae Scientiarum Imperialis Petropolitanae **8** (1736), 128–140 = Opera Omnia (1) 7 (1911–56), 1–10.

[4] W. Hopkins, *The Truth about Königsberg*, The College Mathematics Journal **35** (2004), 198–207.

[5] J.J. Sylvester, *Chemistry and Algebra*, Nature **17** (1878), 284–284.

[6] J. Petersen, *Die Theorie der regulären Graphs*, Acta Mathematica **15** (1891), 193–220.

[7] D. Kőnig, *Theorie der endlichen und unendlichen Graphen. Kombinatorische Topologie der Streckenkomplexe*, Math. u. ihre Anwendung in Monogr. u. Lehrbüchern 16, Akad. Verlagsgesellschaft, Leipzig, 1936.

[8] F.P. Ramsey, *On a problem of formal logic*, Proceedings of the London Mathematical Society **30**(1) (1930), 264–286.

Theorem 1.1 (Ramsey's Theorem, Two-Colour-Version) *Given two complete graphs K_r and K_b ($r, b \geq 2$), one can find a complete graph having the property that with respect to any two-colouring of its edges (e.g. with red and blue) it contains a red K_r or a blue K_b.*

As a special case, we have the simple fact that every graph $G = (V, E)$ with at least six vertices contains a complete triangle, i.e. a three-clique, or the complementary graph $\overline{G} = (V, \overline{E})$ (where $\overline{E}$ consists precisely of those edges between vertices in V which are missing in E) contains a complete triangle, i.e. G contains an independent set of 3 vertices.

Ramsey's theorem was not the first one of its kind. As early as 1927 van der Waerden proved the following result in number theory[9]:

Theorem 1.2 *For any positive integer r there exists a positive integer n and an arithmetic progression P of length r lying in the set $\{1, \ldots, n\}$ such that any function $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, r\}$ restricted to P is constant.*

Now let us reformulate van der Waerden's theorem

- in terms of colours: *For each positive integer r there is an n such that $\{1, \ldots, n\}$ contains a monochromatic arithmetic progression of length r for any r-colouring.*
- in terms of partitions (cf. initial characterization of Ramsey theory): *For each positive integer r there is an n such that at least one subset of any r-partition of $\{1, \ldots, n\}$ contains an arithmetic progression of length r.*

Again and again graph theory and number theory have applied tools from the other discipline to solve problems of their own. A famous example is the following generalization of van der Waerden's theorem, conjectured by Erdős und Turàn in 1936[10]:

Conjecture 1.3 Each set of positive integers having positive natural density contains an arithmetic progression of length k for any k.

This conjecture was proven in 1975 and has been known as *Szemerédi's theorem* ever since. Szemerédi's celebrated proof of this number-theoretic (looking?) assertion used combinatorial and, in particular, graph-theoretic tools.[11] For $k = 3$, the result was established in 1953 by Klaus Roth[12] by adapting the Hardy–Littlewood circle method. Meanwhile, further completely different proofs are known. One of

[9] B.L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. **15** (1927), 212–216.

[10] P. Erdős and P. Turàn, *On some sequences of integers*, Journal of the London Mathematical Society **11**(4) (1936), 261–264.

[11] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Artithmetica **27** (1975), 199–245.

[12] K. Roth, *On certain sets of integers*, Journal of the London Mathematical Society **28**(1) (1953), 104–109.

them, using ergodic theory, was published by Furstenberg,[13] another more recent one by Gowers[14] applies tools from both Fourier analysis and combinatorics. Terence Tao[15] coined the phrase of a *Rosetta stone* to illustrate how various proofs of Szemerédi's theorem connect different fields of mathematics. Green and Tao were the ones who showed that Szemerédi's theorem is not the end of the story. They proved[16] that even the set of prime integers, although having density zero, contains arithmetic progressions of arbitrary length, the reason being that the sequence of primes behaves 'random enough' besides the fact that is it 'not too thin'.

2 Divisibility and Coprimality

Erdős himself pointed out repeatedly how helpful graph theory could be for certain problems in number theory.[17] Quite often graphs can be used to model correlations between integers.[18] Classical examples are *divisor graphs* and *coprime graphs* (also called *relatively prime graphs*).

The vertices of a *divisor graph* are given by the elements of any set of positive integers. Two such integers m and n, say, are considered adjacent if and only if one of them divides the other. Of course, one could refine the model by using a directed graph to distinguish between $m \mid n$ and $n \mid m$. Anyway, the resulting graph models the divisibility relation in the given set. As an example of the benefit of this perspective, Pomerance[19] gained surprising structural insights by investigating longest paths in divisor graphs. Chartrand et al. asked: Which graphs do occur as divisor graphs? More precisely, they investigated for which graphs the vertices can be numbered by different positive integers such that the divisor graph of this set of integers is the given one. Chartrand et al.[20] proved among other things:

[13]H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, Journal d'Analyse Math. **31** (1977), 204–256.

[14]T. Gowers *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11**(3) (2001), 465–588.

[15]T. Tao, *The dichotomy between structure and randomness, arithmetic progressions, and the primes*, pp. 581–608 in: M. Sanz-Solé, J. Soria, J.L. Varona et al., International Congress of Mathematicians Zürich, European Mathematical Society, Zürich, 2007.

[16]B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167**(2) (2008), 481–547.

[17]E.g. P. Erdős, *Some applications of graph theory to number theory*, pp. 77–82 in: *The Many Facets of Graph Theory*, Proc. Conf. Western Mich. Univ., Kalamazoo, Mich. 1968, Springer LNM, Berlin, 1969.

[18]Cf. chapter *Graphs on the integers*, in: R.L. Graham, M. Grötschel, L. Lovász, *Handbook of Combinatorics*, Vol. 1, North-Holland, New York, 1995.

[19]C. Pomerance, *On the longest simple path in the divisor graph*, Congressus Numerantium **40** (1983), 291–304.

[20]G. Chartrand, R. Muntean, V. Saenpholphat, and P. Zhang, *Which graphs are divisor graphs?*, Congressus Numerantium **151** (2001), 189–200.

1. Every complete graph is a divisor graph.
2. Every tree and, more generally, every bipartite graph is a divisor graph.
3. Every induced subgraph of a divisor graph is again a divisor graph.
4. Divisor graphs cannot contain induced circles of odd length greater than 3 (i.e. at most triangles).
5. A graph without triangles is a divisor graph if and only if it is bipartite.

Finally, they gave this elegant characterization:

Theorem 2.1 *A graph is a divisor graph if and only if there exists an orientation of its edges such that every non-isolated vertex v is either source (i.e. v has only outgoing edges) or sink (i.e. v has only incoming edges), or, if v has incoming and outgoing edges, then each incoming neighbour*[21] *of v has edges to each of the outgoing neighbours of v.*

One of the most spectacular results in graph theory was the proof of an old conjecture of Berge, namely the *strong perfect graph theorem*.[22] By using this powerful tool, Al-Addassi et al. showed in 2012 that all divisor graphs are perfect,[23] i.e. the chromatic number of every induced subgraph equals the size of the largest clique of that subgraph. The strong perfect graph theorem implies a weaker statement[24] saying that a graph is perfect if and only if its complement is perfect as well.

As a second example, we shall look at *coprime graphs*. Given a set S of positive integers, the corresponding coprime graph $\mathrm{Copr}(S)$ is defined to have vertex set S and edges between $m, n \in S$ if $\gcd(m, n) = 1$. It is easy to show that every graph is a coprime graph $\mathrm{Copr}(S)$ for a suitable set S[20]. At this point it is natural to shift the focus from the question which graphs are coprime graphs to the correspondence between arithmetical features of S and certain graph properties. For example, Erdős und Sárközy looked for circles in coprime graphs[25] and the existence of complete tripartite subgraphs.[26]

In the literature, one can also find a more restrictive notion of coprime graphs: a graph having n vertices is called a coprime graph if its vertices may be numbered by the integers $1, \ldots, n$ in such a way that all pairs of adjacent vertices are coprime (but

[21] *Neighbour* is synonymously used for adjacent vertex.

[22] M. Chudnovsky, N. Robertson, P. Seymour, and R. Thomas, *The strong perfect graph theorem*, Annals of Mathematics **164**(1) (2006), 51–229.

[23] S. Al-Addasi, O.A. AbuGhneim, and H. Al-Ezeh, *Further new properties of divisor graphs*, J. Comb. Math. Comb. Comput. **81** (2012), 261–272.

[24] As also conjectured by Berge and shown by L. Lovász, (1972), *A characterization of perfect graphs*, Journal of Combinatorial Theory, Series B **13**(2) (1972), 95–98.

[25] P. Erdős and G.N. Sárközy, *On cycles in the coprime graph of integers*, Electron. J. Comb. **4**(2) (1997), Research paper R8.

[26] G.N. Sárközy, *Complete tripartite subgraphs in the coprime graph of integers*, Discrete Mathematics **202** (1999), 227–238.

possibly others as well).[27] With regard to this stronger definition of coprimality, it is no longer obvious which graphs have that property at all. A famous conjecture made by Entringer und Tout in the 1980s says that every tree, i.e. every graph containing no cycles, is a 'strong' coprime graph. For small trees this conjecture has been verified by inspection. More importantly it was shown recently that the conjecture holds for all sufficiently large trees.[28]

Even more specific is the so-called *maximal coprime graph* $\mathrm{Copr}(n) := \mathrm{Copr}(\{1, 2, \ldots, n\})$, defined for every positive integer n (where $a, b \in \{1, \ldots, n\}$ are adjacent if and only if $\gcd(a, b) = 1$. Quite a few structural features of these graphs are known[29]:

- $\mathrm{Copr}(n-1)$ is an induced subgraph of $\mathrm{Copr}(n)$.
- Each spanning subgraph of $\mathrm{Copr}(n)$ is a maximal coprime graph itself.
- Each graph containing a graph which is not maximal coprime has this property as well.

3 Integrality: A First Taste

The integers are the fundamental object of study for number theorists. There is no obvious analogous concept of integrality for graphs. But whenever some graph property is measured with a number set containing integers it is natural to ask for which graphs the property assumes integral values. A prominent case is the spectrum of the adjacency matrix. For a finite graph $G = (V, E)$ with $|V| = \{v_1, \ldots, v_n\}$, say, the adjacency matrix $A(G) = (a_{ij})$ is defined as the $n \times n$ matrix with entries $a_{ij} = 1$ if v_i and v_j are adjacent, and $a_{ij} = 0$ otherwise. Observe that for an undirected graph G the matrix $A(G)$ is a symmetric 0-1-matrix. Linear algebra tells us that all eigenvalues of $A(G)$ are real numbers. Moreover, since every rational eigenvalue of an integer matrix is an integer, any graph eigenvalue is either an integer or an irrational number. The research revolving around eigenvalues and eigenspaces of graphs forms the field of *spectral graph theory*.

A graph G is called an *integral graph* if all eigenvalues of G, which means all eigenvalues of $A(G)$, are integers. In other words, integral graphs have an integral spectrum. The problem to characterize all integral graphs was first raised in 1974 by

[27] This procedure is named *coprime labelling* or, rather unsuitably, *prime labelling*.

[28] P. Haxell, O. Pikhurko, and A. Taraz, *Primality of trees*, J. Comb. **2**(4) (2011), 481–500.

[29] See the survey article by S.N. Rao, *A Creative Review on Coprime (Prime) Graphs*, Lecture Notes, DST Work Shop (23–28 May 2011), WGTA, BHU, Varanasi, 2011.

Harary and Schwenk.[30] Since then many partial answers to this apparently difficult question have been published.[31]

Before considering integrality itself, let us consider an example that demonstrates how even the question whether a graph exhibits a certain integer in its spectrum leads to interesting insights. To this end, let us take a closer look at the spectrum of the maximal coprime graph $\mathrm{Copr}(n)$. While numerical experiments quickly reveal that $\mathrm{Copr}(n)$ might not be integral, they also suggest that the integer 0 always belongs to the spectrum. Moreover, one is lead to conjecture that the multiplicity of 0 in the spectrum increases monotonously as n grows. Since $\gcd(1,1) = 1$, each coprime graph has a loop at 1. This we agree to remove in order to have a *loopless coprime graph* (this does not influence essentially what follows). The authors[32] proved the following:

Theorem 3.1 *For any integer $n > 1$, the geometric multiplicity $\gamma(n)$ of the eigenvalue 0 of the loopless coprime graph* $\mathrm{Copr}(n)$ *satisfies*

$$\gamma(n) = \begin{cases} \nu(n) & \text{if } M(n) \neq 1, \\ \nu(n) + 1 & \text{if } M(n) = 1, \end{cases}$$

where $\mu(n)$ denotes the Moebius function, $\nu(n) := n - \sum_{k \leq n} |\mu(k)|$, and $M(n) := \sum_{k=1}^{n} \mu(k)$ is Mertens' function. Consequently,

$$\gamma(n) = \left(1 - \frac{6}{\pi^2}\right) n + O(\sqrt{n}).$$

Moreover, it turned out that in case $M(n) \neq 1$ the kernel of the loopless $\mathrm{Copr}(n)$ has a so-called *simple basis* containing vectors with no other entries than $0, 1, -1$. This is wrong if $M(n) = 1$. In comparison, the coprime graphs with loop at 1 always have a simple kernel basis.

4 Graph and Groups: Even More Integrality

Another class of graphs related to algebra and, in particular, to number theory are *Cayley graphs*. Generally, these graphs model algebraic relations between elements of groups (or rings). Given a (finite) group H, the Cayley graph $\mathrm{Cay}(H, S)$ has vertex set H, and we need a so-called set $S \subseteq H$ of *symbols*. Assuming H to be an additive

[30] F. Harary and A.J. Schwenk, *Which graphs have integral spectra?*, pp. 45–51 in: *Graphs and Combinatorics*, Springer, Berlin, 1974.

[31] K. Balinska, D. Cvetkovic, Z. Radosavljevic, S. Simic, and D. Stevanovic, *A survey on integral graphs*. Publ. Elektroteh. Fak., Univ. Beogr., Ser. Mat. **13** (2002), 42–65.

[32] J.W. Sander and T. Sander, *On the kernel of the coprime graph of integers*, Integers **9** (2009), 569–579.

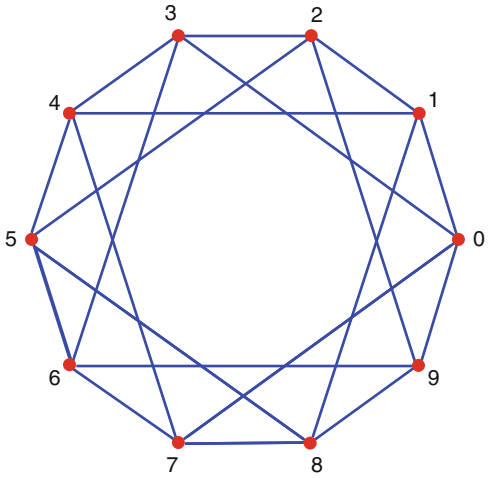


Fig. 1 $\mathrm{Cay}(\mathbb{Z}_{10}, \mathbb{Z}_{10}^*) = \mathrm{Cay}(\mathbb{Z}_{10}, \{1, 3, 7, 9\}) = \mathrm{UCay}(10) = \mathrm{ICG}(10, \{1\})$

group $(H, +)$, S is required to satisfy $0 \notin S$ and $S = -S := \{-s : s \in S\}$ (for multiplicative groups $(H, \cdot)$, we require $1 \notin S$ and $S = S^{-1} := \{s^{-1} : s \in S\}$ correspondingly). Two vertices $x, y \in H$ are defined to be adjacent if $x - y \in S$ (or $xy^{-1} \in S$, respectively). By the conditions on S, Cayley graphs are loopless and undirected (Fig. 1).

The research on Cayley graphs has been extensive and diverse.[33] One of the most basic structural problems asks for isomorphic Cayley graphs, where two graphs $G = (V, E)$ und $G' = (V', E')$ in general are called *isomorphic* if there is a bijection $\varphi : V \to V'$ satisfying $(x, y) \in E \Leftrightarrow (\varphi(x), \varphi(y)) \in E'$. Trivially, each Cayley graph $\mathrm{Cay}(H, S)$ is isomorphic to $\mathrm{Cay}(H, aS)$ by way of the translation $\varphi(x) = ax$. More generally, every group automorphism σ on H yields an isomorphism between $\mathrm{Cay}(H, S)$ und $\mathrm{Cay}(H, \sigma(S))$. The inverse problem to determine if there is an isomorphism between two given graphs is much harder. Even the task to find explicit criteria for isomorphy between graphs in very simple subclasses of Cayley graphs took decades.[34]

4.1 Circulant Graphs

As an example closer related to number theory, let us consider the class of *circulant graphs*. These are the Cayley graphs over cyclic groups (i.e. over some additive

[33] G. Hahn and G. Sabidussi, *Graph symmetry: algebraic methods and applications*, Proceedings of the NATO Advanced Study Institute and séminaire de mathématiques supérieures, Montréal, Canada, July 1–12, 1996; Springer, New York, 1997.

[34] C.H. Li, *On isomorphisms of finite Cayley graphs—a survey*, Discrete Mathematics **256**(1–2) (2002), 301–334.

group $(\mathbb{Z}_n, +)$ of residue classes mod n; cf. Fig. 1). Their adjacency matrices are *circulant matrices*, which have been studied for quite some time.[35] A first important result on the isomorphy between circulant graphs was published in 1967, however, only in case the graphs have prime order, i.e. the number of vertices is a prime number[36]:

Theorem 4.1 *Let p be prime. Then* $\mathrm{Cay}(\mathbb{Z}_p, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_p, S')$ *are isomorphic if and only if there exists a unit $a \in \mathbb{Z}_p^*$ such that $S' = aS$.*

This shows that among circulant graphs of prime order only the trivial isomorphisms by translation exist. In other words, checking two such graphs for isomorphy can be reduced to comparing the two sets of symbols. Unfortunately, this easy reduction does not work for circulant graphs over $\mathbb{Z}_n$ with arbitrary n[37]:

Theorem 4.2 *If* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *are isomorphic, then there exists an isomorphism by translation if and only if $n \in \{8, 9, 18\}$ or $n = 2^e m$ with $e \in \{0, 1, 2\}$ and m odd and squarefree.*

Tremendous efforts were made to find a manageable criterion for isomorphy between circulant graphs in general (in analogy to Theorem 4.1), which allows to characterize isomorphic circulant graphs by explicit comparison of their symbol sets. This was finally proven at the turn of the millennium, and it became apparent that the comparison of the two symbol sets has to be performed in 'layers'. The *d-th layer* $(S)_d$ of a symbol S in a group of order n is defined by $(S)_d = \{s \in S : \gcd(s, n) = d\}$, and we have

Theorem 4.3 $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *are isomorphic if and only if for each $d|n$ there exists an integer $m_d \in \mathbb{Z}_n^*$ such that $m_d(S)_d = (S')_d$.*

This result had been conjectured in 1975 by D.K. Zibin, and it was confirmed in 2001/2002 independently by two research teams.[38] The criterion reveals that isomorphy is related to certain divisibility properties of the elements of the symbol sets.

In a similar fashion, another arithmetic criterion exists to characterize *connectivity* of Cayley graphs. In fact, a general Cayley graph $\mathrm{Cay}(H, S)$ is connected if and only if the symbol set S generates the group H. Consequently, a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ with $S = \{s_1, \ldots, s_k\}$ is connected if and only if $\gcd(n, s_1, \ldots, s_k) = 1$. More precisely, such a circulant graph satisfying $\gcd(n, s_1, \ldots, s_k) = d$ decomposes

[35] Ph.J. Davis, *Circulant matrices*, Pure and applied Mathematics. Wiley-Interscience Publication, New York, 1979; 2nd ed., AMS Chelsea Publishing, 1994.

[36] J. Turner, *Point-Symmetric Graphs with a Prime Number of Points*, Journal Comb. Theory **3** (1967), 136–145.

[37] This is a result of Muzychuk, to be found in Hahn/Sabidussi.[33]

[38] M. Muzychuk, M. Klin, and R. Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory*, (DIMACS workshop 1999), Ser. Discrete Math. Theor. Comput. Sci. **56** (2001), 241–264; and E. Dobson and J. Morris, *Toida's conjecture is true*, Electron. J. Comb. **9**(1) (2002), Research paper R35.

into exactly d isomorphic graph components $\mathrm{Cay}(\mathbb{Z}_{n/d}, S)$. For Cayley graphs in general the components are $\mathrm{Cay}(\langle S\rangle, S)$.

Circulants form an important class of graphs having many applications in different fields, e.g. in redundant network modelling,[39] where the simplest cases are *powers* $C_n^{(k)}$ *of cycle graphs* C_n with symbol set $\{-k, -k+1, \ldots, -1, 1, \ldots, k-1, k\}$. Circulant graphs are also related to physics, since they model the behaviour of quantum systems. Such a system turns out to be periodic if and only if the corresponding graph is integral.[40]

The eigenvalues of circulant graphs, i.e. the eigenvalues of circulant matrices, can be computed by a handy formula (cf. Davis[35]). Setting $\omega_n = \exp(2i\pi/n)$, the eigenvalues λ_j of $\mathrm{Cay}(\mathbb{Z}_n, S)$ are given by

$$\lambda_j = \sum_{s\in S} \omega_n^{js}, \quad j = 0, \ldots, n-1. \tag{4.1}$$

Then $v_j := (\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1})^T$ is a complex-valued eigenvector for λ_j, and the vectors $v_0, \ldots, v_{n-1}$ are a basis of $\mathbb{R}^n$. Two questions come to mind: In which cases is the circulant graph, i.e. its spectrum, integral? What about real eigenvectors?

To answer the first question, the layers of the symbol set S (see Theorem 4.3) play the decisive role: $\mathrm{Cay}(\mathbb{Z}_n, S)$ is integral if and only if S is made up of complete layers. If we define $G_n(d) = \{s \in \mathbb{Z}_n^* : \ \gcd(s, n) = d\}$ we have[41]:

Theorem 4.4 *A circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is integral if and only if there exists a set* D *of divisors of* n *such that* $S = \bigcup_{d\in D} G_n(d)$.

Consequently, integral circulant graphs are characterized by simply stating n and D. Therefore one may define the graph $\mathrm{ICG}(n, D)$ as the graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ with

$$S = \bigcup_{d\in D} G_n(d) = \{s \in \mathbb{Z}_n^* : \gcd(s, n) \in D\}. \tag{4.2}$$

A special subclass of circulant graphs are the *unitary Cayley graphs* $\mathrm{UCay}(n) := \mathrm{Cay}(\mathbb{Z}_n, G_n(1))$ (Fig. 1). The name is derived from the fact that $G_n(1) = \mathbb{Z}_n^*$ is the group of units in the ring $\mathbb{Z}_n$. Using the preceding theorem and some easy number-theoretic arguments, the integrality of unitary Cayley graphs can be shown as follows. According to the special structure of its symbol set, the eigenvalues of $\mathrm{UCay}(n)$ are

$$\lambda_r \ = \sum_{\substack{1\le j<n \\ \gcd(j,n)=1}} w^{rj} \ = \ c(r, n) \quad \text{for } 0 \le r \le n-1\,.$$

[39] C.K. Wong and D. Coppersmith, *A combinatorial problem related to multimodule memory organizations*, J. Assoc. Comput. Mach. **21** (1974), 392–402.

[40] N. Saxena, S. Severini, and I.E. Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, Int. J. Quantum Inf. **5**(3) (2007), 417–430.

[41] W. So, *Integral circulant graphs*, Discrete Mathematics **306** (2005), 153–158.

Here $c(r,n)$ is a *Ramanujan sum*, which is known to be integer-valued for all $r,n > 0$. Thus unitary Cayley graphs are integral, and their eigenvalues can be computed by[42]

$$\lambda_r \;=\; c(r,n) \;=\; \mu(t_r)\frac{\varphi(n)}{\varphi(t_r)},\ \text{where } t_r = \frac{n}{\gcd(r,n)} \quad \text{for } 0 \le r \le n-1,$$

μ again denotes the Möbius function, and φ is Euler's totient function. It is an immediate consequence of this formula that each eigenvalue $\lambda \neq 0$ of $\mathrm{UCay}(n)$ is a divisor of $\varphi(n)$.

With regard to the characterization of the eigenvalues of unitary Cayley graphs in terms of Ramanujan sums it is not difficult to see that, more generally, every graph $\mathrm{Cay}(\mathbb{Z}_n, G_n(d))$ is indeed integral. Uniting the symbol sets of such graphs yields a partition of the sum in (4.1) accordingly. This implies that the eigenvalues of each such graph are sums of the eigenvalues of the graphs $\mathrm{Cay}(\mathbb{Z}_n, G_n(d))$. By this argument we have obtained one direction of the assertion in Theorem 4.4. The other direction requires more effort.

4.2 Moving on to Integral Cayley Graphs

In view of Eq. (4.2) one can define a superclass of the integral circulants.[43] First fix a finite abelian group H of order n. Here we may assume $H = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$ for suitable $m_1 \cdot \ldots \cdot m_r = n$ with $\gcd(m_i, m_j) \le 2$ (for all $i \neq j$). We define a tuple-wise greatest common divisor of given tuples $x = (x_1, \ldots, x_n)$ and $m = (m_1, \ldots, m_n)$ by

$$\gcd(x,m) = (d_1, \ldots, d_r) \text{ with } d_i = \gcd(x_i, m_i),$$

agreeing on $\gcd(0,m) := m$. Armed with this definition, the definition of the sets $G_n(d)$ readily extends to the new context (with respect to the chosen representation of H).

The sets $G_n(d)$ can be viewed as layers of integral symbol sets with respect to $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$. More precisely, the sets $G_n(d)$ generate a Boolean algebra $B_{\gcd}(H)$ with respect to intersection, union and complement of sets. Using the elements of $B_{\gcd}(H)$ as symbols, they all give rise to integral Cayley graphs on H. One can show that $B_{\gcd}$ is a subalgebra of the Boolean algebra $B(H)$ that is generated by the subgroups of H (tacitly removing the neutral element of H from each set). Note that

[42] See, e.g., P.J. McCarthy, *Introduction to arithmetical functions*, Universitext, Springer, New York, 1986.

[43] W. Klotz and T. Sander, *Integral Cayley graphs defined by greatest common divisors*, Electron. J. Comb. **18**(1) (2011), Research paper P94.

$S = S^{-1}$ for all sets $S \subseteq B(H)$ so that they indeed constitute valid symbols. Actually, all of the elements of the Boolean algebra $B(H)$ give rise to integral Cayley graphs on H.[44]

The *Sudoku graphs* are interesting examples of integral Cayley graphs. The board of an n-Sudoku consists of a square arrangement of cells, with n^2 rows and n^2 columns. The board is subdivided into an n times n arrangement of square blocks with n^2 cells each. Successfully solving a (possibly pre-filled) n-Sudoku means assigning integers 1 to n to the cells in such a way that each row, cell and block contains distinct numbers. For $n = 3$ we obtain the classical Sudoku we know from our daily newspapers.

Let us construct a graph associated with an n-Sudoku board. The Sudoku graph $\mathrm{Sud}(n)$ has n^4 vertices, representing the distinct cells of the board. Two vertices are adjacent if and only if they represent cells that are located in the same row, column or block. So the Sudoku graph represents the requirement of filling in distinct numbers. Consequently, solving an n-Sudoku puzzle is equivalent to finding a proper n-coloring of the graph $\mathrm{Sud}(n)$.

The vertex set of $\mathrm{Sud}(n)$ may be identified with $\mathbb{Z}_n^4$. Let us assume that each vertex (x_1, x_2, x_3, x_4) encodes the position of its associated cell as follows: (x_1, x_2) locates the block, by using x_1 as horizontal and x_2 as vertical position index with respect to the block grid; (x_3, x_4) works in a similar fashion and locates the cell within the selected block. Then we have[45]:

Theorem 4.5 $\mathrm{Sud}(n) \simeq \mathrm{Cay}(\mathbb{Z}_n^4, S_1 \dot\cup S_2 \dot\cup S_3)$ *for*

$$\begin{aligned} S_1 &= \{(0,0,x_3,x_4) : x_3, x_4 \in \mathbb{Z}_n,\ (x_3,x_4) \neq (0,0)\} \\ &= (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_n \times \mathbb{Z}_n) \setminus (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_1), \\ S_2 &= \{(0,x_2,0,x_4) : x_2, x_4 \in \mathbb{Z}_n,\ x_2 \neq 0\} \\ &= (\mathbb{Z}_1 \times \mathbb{Z}_n \times \mathbb{Z}_1 \times \mathbb{Z}_n) \setminus (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_n), \\ S_3 &= \{(x_1,0,x_3,0) : x_1, x_3 \in \mathbb{Z}_n,\ x_1 \neq 0\} \\ &= (\mathbb{Z}_n \times \mathbb{Z}_1 \times \mathbb{Z}_n \times \mathbb{Z}_1) \setminus (\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_n \times \mathbb{Z}_1). \end{aligned}$$

We see that Sudoku graphs are indeed integral Cayley graphs—the sets S_i are (disjoint) subgroups of H (neglecting the neutral element), so their union belongs to $B(\mathbb{Z}_n^4)$.

[44] W. Klotz and T. Sander, *Integral Cayley graphs over Abelian groups*, Electron. J. Comb. **17**(1) (2010), Research paper R81.

[45] W. Klotz and T. Sander, *Wie kommt Sudoku zu ganzzahligen Eigenwerten?* (*How does Sudoku acquire integral eigenvalues?*), Math. Semesterber. **57**(2) (2010), 169–183.

4.3 Having the Right Tools

In many papers concerning integrality of Cayley graphs, group characters are a frequently employed tool. A character is a homomorphism of a group into the multiplicative group of $\mathbb{C} \setminus \{0\}$. The use of group characters is induced by the fact that Cayley graphs are *vertex transitive*.[46] It follows directly from the definition of a Cayley graph that the translations of its group do the trick here. Consequently, for spectral studies of Cayley graphs, one can employ a method outlined in a 1975 paper by Lovász.[47] When applied specifically to Cayley graphs, the method looks as follows. Let H be a finite group and ψ a character of H. Defining

$$\psi(S) = \sum_{s \in S} \psi(s),$$

note that

$$\sum_{x \in N(v)} \psi(x) = \psi(S)\psi(v)$$

for every vertex v of $\mathrm{Cay}(H, S)$, where $N(v)$ is the *neighbourhood*[48] of v. It follows that, for any given symbol S, the function ψ is an eigenfunction of the graph $\mathrm{Cay}(H, S)$ for eigenvalue $\psi(S)$. More generally, one can look for sets T such that $\psi(T) \in \mathbb{Z}$ for all n characters ψ of the given group H.

4.4 Diving Deeper into Integrality

Let us investigate the mutual relation of the Boolean algebras $B_{\gcd}(H)$ and $B(H)$, for finite abelian groups H. One can show that equality $B_{\gcd}(H) = B(H)$ holds if and only if H can be represented in the form $H = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \times \mathbb{Z}_{\geq 2}$[50]. A Cayley graph on such a group H is integral if and only if its symbol set belongs to the Boolean algebra $B(H)$. So here integrality is once again characterized by a certain composition of the symbol set.

This takes us to the question of how to identify all symbol sets giving rise to integral Cayley graphs on some fixed group H. To this end, let us take a closer look at the involved Boolean algebras. How can they be generated? If H is a finite abelian group of order n, again represented as a suitable product of cyclic groups,

[46] Vertex transitive graphs are exactly those graphs whose automorphism group acts transitively on its vertex set. In other words, for any two vertices there needs to exist an automorphism mapping the first vertex to the second.

[47] L. Lovász, *Spectra of graphs with transitive groups*, Period. Math. Hung. **6** (1975), 191–195.

[48] I.e. the set of all vertices adjacent to v.

then each element of $B_{\gcd}(H)$ is a disjoint union of the layers $G_n(d)$. These layers are the *atoms*[49] of $B_{\gcd}(H)$.

Actually, also the enclosing algebra $B(H)$ is atomic, for any finite (not necessarily abelian) group H. Its atoms are exactly the generators of the cyclic subgroups of H. Each such atom gives rise[50] to an integral Cayley graph on H. As an example, consider the cyclic group $\mathbb{Z}_{24}$. We have $G_{24}(4) = \{4, 20\}$. This is an atom of $B(\mathbb{Z}_{24})$ since its elements generate the cyclic subgroup $\langle 4\rangle$ of $\mathbb{Z}_{24}$.

The collection of all symbol sets S for which $\mathrm{Cay}(H, S)$ is integral forms yet another Boolean algebra. Let us denote it by $B_{\mathrm{Int}}(H)$. Obviously, the atoms of $B(H)$ are also elements of $B_{\mathrm{Int}}(H)$. Hence $B(H)$ is a subalgebra of $B_{\mathrm{Int}}(H)$. Effectively, $B(H)$ is generated by a subset of the atoms of $B_{\mathrm{Int}}(H)$. In the case of finite abelian groups H it turns out, however, that both algebras coincide[50]:

Theorem 4.6 *If H is a finite abelian group, then*

$$B_{\mathrm{Int}}(H) = B(H).$$

So a Cayley graph on a finite abelian group H is integral if and only if its symbol set is a union of complete generating sets of cyclic subgroups of H. This fact is a beautiful extension of Theorem 4.4.

The structure of the Boolean algebra $B_{\mathrm{Int}}(H)$ has been studied quite well[51]:

Theorem 4.7 *Let H be a finite group with center C. Then the power set $P(H - C)$ constitutes a Boolean subalgebra of $B_{\mathrm{Int}}(H)$. Moreover, $B_{\mathrm{Int}}(H)$ is a direct product of $B(C)$ and $P(H - C)$.*

An immediate and important consequence of this theorem is that $B_{\mathrm{Int}}(H) = B(H)$ can only hold if the finite group H is abelian. So we know the limits of atomic construction of symbol sets.

An interesting side question is whether there exist groups such that any symbol readily gives rise to an integral Cayley graph. Such groups are called *Cayley integral*. It turns out that Cayley integral groups are scarce. The nontrivial abelian Cayley integral groups are represented by[44]

$$\mathbb{Z}_2^m \times \mathbb{Z}_3^n,\ \mathbb{Z}_2^m \times \mathbb{Z}_4^n,\quad m, n \geq 0.$$

[49] An element a of a lattice with associated partial order $\leq$ and least element 0 is an *atom* if $0 < a$ and no element x satisfies $0 < x < a$. A lattice is *atomic* if, for every element $b \neq 0$, we have $a \leq b$ for some atom a.

[50] R.C. Alperin and B.L. Peterson, *Integral sets and Cayley graphs of finite groups*, Electron. J. Comb. **19**(1) (2012), Research paper P44.

[51] R.C. Alperin and B.L. Peterson, *Integral sets and the center of a finite group*, Can. Math. Bull. **57**(1) (2014), 9–11.

In the non-abelian case the list is

$$S_3,\ \mathbb{Z}_3 \rtimes \mathbb{Z}_4,\ Q_8 \times \mathbb{Z}_2^n,\ \ n \geq 0,$$

where S_3 is the symmetric group of order 3, the semidirect product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ is the dicyclic group of order 12 and Q_8 is the quaternion group of order 8. Coincidentally, the latter list has been discovered twice, independently and almost simultaneously.[52]

4.5 Playing with Atoms

Returning to the Boolean algebra $B(H)$, let us take a closer at its atoms and generating sets of cyclic groups in general. Here, interesting number-theoretic questions arise that can be investigated even beyond the graph-theoretic context. Fix a finite abelian group H and define

$$\text{atom}(a) := \{a' :\ \langle a' \rangle = \langle a \rangle\}.^{53} \tag{4.3}$$

Let us assume in the following that H is an additive group $(H, +)$. What happens if we add two atoms? More precisely, we ask about the structure of the set $\text{atom}(a) + \text{atom}(b)$, where the set sum is defined in the usual way

$$M_1 + M_2 := \{m_1 + m_2 :\ m_1 \in M_1,\ m_2 \in M_2\}$$

for given sets M_1 and M_2. Surprisingly, it turns out that $\text{atom}(a) + \text{atom}(b) \in B(H)$ for any given pair $a, b \in H$.[54] With respect to Cayley graphs we see that sums of atoms give rise to integral Cayley graphs. This comes in handy when studying *distance powers*[55] of integral Cayley graphs. Distance powers of Cayley graphs are again Cayley graphs. It is not difficult to see that the symbol set of such a distance power is formed by successive addition of symbols of the original Cayley graph. Consequently, such a symbol set is a sum of (disjoint unions of) atoms. Hence it gives rise to an integral Cayley graph.

In essence, any distance power is an overlay of d graphs where each contains exactly the edges representing distance d. Each individual layer is an integral Cayley graph in itself. Taking this construction to the extreme, one can even do

[52] A. Abdollahi and M. Jazaeri, *Groups all of whose undirected Cayley graphs are integral*, European Journal of Combinatorics **38** (2014), 102–109; and A. Ahmady, J.P. Bell, and B. Mohar, *Integral Cayley graphs and groups*, SIAM J. Discrete Math. **28**(2) (2014), 685–701.

[53] This definition coincides with the concept of atoms in Boolean algebras discussed before.

[54] W. Klotz and T. Sander, *Distance powers and distance matrices of integral Cayley graphs over abelian groups*, Electron. J. Comb. **19**(4) (2012), Research paper P25.

[55] The d-th distance power $G^{(d)}$ of a graph G has the same vertex sets as G. Two vertices $x \neq y$ are joined by an edge if and only if their distance in G is at most d.

the following: Fix a function $m : \mathbb{N} \to \mathbb{N}_0$ of multiplicities and construct a weighted distance power multigraph by having exactly $m(d)$ edges between any two vertices of distance d. The result is an integral graph.

For cyclic groups the sum of atoms has been studied even further, leading to interesting topics of number theory. Given a finite abelian group H and an element $a \in H$, we have $\mathrm{atom}(a) = \{a' \in H : \ \langle a' \rangle = \langle a \rangle\}$ as in (4.3). Viewing $\mathbb{Z}_n$ in the context of the residue class ring $\mathbb{Z}/n\mathbb{Z}$ we see that the cyclic subgroup $\langle a \rangle$ of the additive group $\mathbb{Z}_n$ simply is the principal ideal $(a) := a\mathbb{Z}_n$ generated by a. So the previous equation translates to

$$\begin{aligned} \mathrm{atom}(a) &= \{au : \ 1 \le u \le n, \ (u, n) = 1\} \\ &= \{ax : \ 1 \le x \le \mathrm{ord}(a), \ (x, \mathrm{ord}(a)) = 1\}, \end{aligned}$$

where $\mathrm{ord}(a) = \frac{n}{(a,n)}$ denotes the order of a in the additive group $\mathbb{Z}_n$

Beyond merely claiming that $\mathrm{atom}(a) + \mathrm{atom}(b)$ is a disjoint union of atoms, one can precisely state for each element $\gamma \in \mathrm{atom}(a) + \mathrm{atom}(b)$ its exact number[56] of possible sum representations $\alpha + \beta$, with $\alpha \in \mathrm{atom}(a)$, $\beta \in \mathrm{atom}(b)$. This has been generalized to sums of any number of atoms,[57] and to abelian groups.[58]

5 Primality

There is indeed a concept of primality in graphs. For this purpose it is convenient to assume the graphs to be *friendly* in the sense that they are undirected, connected and without *leaves*, i.e. without vertices having just one neighbour. Friendly graphs G contain cycles,[59] and each closed walk which is not the repetition of a shorter closed walk is called a *prime* in G.[60] Let us illustrate the concept by an example, where the graph G simply consists of two cycle graphs C_1 and C_2, say, which have exactly one vertex v in common. Then both C_1 and C_2 are primes in G, but walks two or more times along C_1 or along C_2 are not. However, a walk starting at v,

[56] J.W. Sander and T. Sander, *Adding generators in cyclic groups*, J. Number Theory **133**(2) (2013), 705–718.

[57] Q.-H. Yang and M. Tang, *On the addition of squares of units and nonunits modulo n*, J. Number Theory **155** (2015), 1–12.

[58] M. Kreh, *Adding generators in abelian groups*, to appear in J. Algebra and Number Theory Acad.

[59] This follows from the fact that trees, by definition, are the cyclefree graphs and must have leaves.

[60] Here we disregard the technical obstacles of *orientation* and *backtracks*, but one can find all details of the precise definition of primes in graphs—and most of the other facts of this section—in A. Terras, *Zeta Functions of Graphs—A Stroll through the Garden*, Cambridge studies in advanced mathematics, Cambridge University Press, Cambridge, 2011, or the first author's *Arithmetical Topics in Algebraic Graph Theory*, in: K. Bringmann, Y. Bugeaud, T. Hilberdink, J.W. Sander, *Four Faces of Number Theory*, European Mathematical Society, Lectures in Mathematics, Zürich, 2015.

following C_1 twice and then running along C_2 once is a prime, while a walk along C_1, C_2, C_1, C_2 is not (since it is the repetition of the prime walk C_1, C_2). All walks $C_1, C_2, C_2, \ldots, C_2$ are apparently primes.

If P is a prime in G, we denote by $\nu(P)$ the length of the corresponding walk and call it the *length of the prime*. It is easy to see that a friendly graph which is not a cycle itself contains at least two different cycle subgraphs and thus infinitely many primes, obtained by taking 'non-periodic' walks using at least two of the cycle subgraphs. Let $\mathbb{P}_G$ be the set of primes in G. Then

$$\pi_G(k) := \#\{P \in \mathbb{P}_G : \ \nu(P) = k\}$$

is called the *prime counting function*.[61] A crucial parameter with respect to $\pi_G(k)$ is $\Delta_G := \gcd\{\nu(P) : \ P \in \mathbb{P}_G\}$, since we clearly have $\pi_G(k) = 0$ in case $\Delta_G \nmid k$.

The *Riemann zeta-function* encodes information about the distribution of primes in the set of positive integers and can be used to prove the *prime number theorem*. The equivalent for primes in graphs and the prime counting function π_G is the *Ihara zeta-function*, first defined by Yasutaka Ihara[62] in the 1960s in the context of discrete subgroups of the two-by-two p-adic special linear group. In his book *Arbres, Amalgames, SL_2*[63] Serre suggested in 1977 that Ihara's original definition could be reinterpreted graph-theoretically.[64] In 1985 Toshikazu Sunada[65] put this suggestion into practice and defined the *Ihara zeta-function* of a friendly graph G as the complex function

$$\zeta_G(u) := \prod_{P \in \mathbb{P}_G} \left(1 - u^{\nu(P)}\right)^{-1},$$

where $u \in \mathbb{C}$ is supposed to have sufficiently small absolute value for reasons of convergence. As other zeta-functions, the Ihara zeta-function satisfies a functional equation[66] and, in addition, the so-called *determinant formulae*, depending on the *edge adjacency matrix* W_G[67] of the graph G. It turns out that the absolute value of the largest eigenvalue of W_G equals the reciprocal of the radius R_G of convergence of ζ_G. Let us denote by Λ_G the second largest modulus of the eigenvalues of W_G.

[61] Observe the $=$ sign as opposed to $\leq$ in the prime counting function for integers.

[62] Y. Ihara, *On discrete subgroups of the two by two projective linear group over p-adic fields*, J. Math. Soc. Japan. **18** (1966), 219–223.

[63] = J.-P. Serre, *Trees*, Springer, New York, 1980.

[64] Namely, as a zeta-function related to closed geodesics in graphs—compare this with Selberg zeta-functions.

[65] T. Sunada, *Riemannian coverings and isospectral manifolds*, Ann. Math. **121** (1985), 169–186.

[66] In fact, there exist several functional equations for $\zeta_G(u)$

[67] W_G is a 0-1-matrix indicating if a pair (e_i, e_j) of edges in G is a path (of length 2) in the graph or not. In other words, the edge adjacency matrix of G is the adjacency matrix of the *line graph* of G, which is obtained from G by exchanging the roles of vertices and edges. For a precise definition look into the books cited in footnote 60.

By somewhat imitating methods from analytic number theory to prove the classical prime number theorem,[68] one obtains the *prime number theorem for graphs*[69]:

Theorem 5.1 *Let G be a friendly graph, and let k be a positive integer. If $\Delta_G \nmid k$, then $\pi_G(k) = 0$. For $\Delta_G \mid k$, we have*

$$\pi_G(k) = \Delta_G \frac{R_G^{-k}}{k} + \mathrm{O}\Big(\frac{\Lambda_G^k}{k}\Big) + \mathrm{O}\Big(\frac{R_G^{-\frac{k}{2}}}{k}\Big). \tag{5.1}$$

In particular, we have $\pi_G(k) \sim \Delta_G \frac{R_G^{-k}}{k}$ asymptotically for $\Delta_G \mid k$ with $k \to \infty$.

It is well known that the *Riemann hypothesis* (for the Riemann zeta-function) implies the best possible error term in the prime number theorem for integers. There exists a corresponding Riemann hypothesis on the location of the zeros of the Ihara zeta-function. Looking at formula (5.1), it becomes clear that best possible error terms are obtained for graphs G for which the *spectral gap* between the largest eigenvalue of W_G (which equals R_G^{-1}, as mentioned above) and the second largest eigenvalue Λ_G of W_G is as big as possible. For a *regular* graph,[70] the spectrum of its edge adjacency matrix is closely related to the spectrum of its (vertex) adjacency matrix.[71] In particular, the corresponding spectral gaps between largest and second largest eigenvalues are correlated. Having all this in mind, the following fact seems not to be very surprising: Among all friendly graphs G, at least if they are *q-regular*, the ones whose Ihara zeta-function satisfies the corresponding Riemann hypothesis are exactly those for which the spectral gap with regard to the adjacency matrix $A(G)$ is as large as possible. Observe that q-regular graphs have largest eigenvalue q in modulus.[72]

By a result of Alon and Boppana[73] we know for q-regular graphs G that the second largest eigenvalue $\Lambda(G)$ in modulus cannot be essentially smaller than $2\sqrt{q-1}$. Graphs where $\Lambda(G) \leq 2\sqrt{q-1}$ are known as *Ramanujan graphs*.[74] Therefore, the Riemann hypothesis for the Ihara zeta-function of a graph G holds precisely if G is a Ramanujan graph.

[68] But with less difficulties and, therefore, much less effort.

[69] For all the details, see the two books mentioned in footnote 60.

[70] A graph is called *q-regular* if every vertex has exactly q neighbours.

[71] I.e. given the spectrum of any regular graph, the spectrum of its line graph can be explicitly specified. This follows from a result of Sachs, see, e.g., Theorem 3.8 in: N. Biggs, *Algebraic graph theory*, 2nd ed., Cambridge University Press, Cambridge, 1993.

[72] This is an exercise in algebraic graph theory.

[73] N. Alon, *Eigenvalues and expanders*, Combinatorica **6** (1986), 83–96, and R.B. Boppana, *Eigenvalues and graph bisection: an average case analysis*, pp. 280–285 in: Proc. 28th Annual Symp. Found. Comp. Sci., IEEE 1987.

[74] For a survey, see M.R. Murty, *Ramanujan graphs*, J. Ramanujan Math. Soc. **18** (2003), 33–52.

Ramanujan graphs are a class of special *expander graphs*,[75] having applications in communication network theory[76] and theoretical computer science.[77] In 1988 Lubotzky et al.[78] constructed an infinite family of $(q+1)$-regular Ramanujan graphs (with growing number of vertices) for each prime $q \equiv 1 \bmod 4$. Their proof used the *Ramanujan conjecture*, which led to the name of Ramanujan graphs. Morgenstern[79] extended the construction of Lubotzky et al. to all prime powers in 1994. The problem of such an explicit construction for general q is open.

6 Multiplicativity

Arithmetical functions[80] were one of Wolfgang Schwarz's main research areas, and multiplicativity is the most important and useful number-theoretic property such a function can have. As we shall see, the concept of multiplicativity is also profitable with respect to certain graph-theoretical problems.

In 1978 Gutman[81] established the mathematical notion of the *energy*

$$E(G) := \sum_{\lambda \in \mathrm{Spec}(G)} |\lambda|. \tag{6.1}$$

of a graph G as the sum of the absolute values of all eigenvalues of G (counted with multiplicities). This terminology has its roots in mathematical chemistry way back in the 1930s and is related to certain chemical parameters, e.g. the heat of formation of a hydrocarbon.[82] By now this concept of graph energy, which is accompanied

[75] Expander graphs have the following two competing properties: on the one hand, they are fairly *sparse* (in terms of number of edges as compared to the number of vertices), but on the other hand, they are *highly connected*. For a formal definition as well as results and applications, see S. Hoory, N. Linial, and A. Widgerson, *Expander graphs and their applications*, Bulletin (New series) of the American Mathematical Society **43**(4) (2006), 439–561.

[76] F. Bien, *Construction of Telephone Networks by Group Representations*, Notices of the Amer. Math. Society **36**(1) (1989), 5–22.

[77] See Hoory et al., footnote 75.

[78] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[79] M. Morgenstern, *Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q*, J. Combinatorial Theory, Series B **62** (1994), 44–62.

[80] W. Schwarz and J. Spilker, *Arithmetical functions: An Introduction to Elementary and Analytic Properties of Arithmetic Functions and to Some of their Almost-Periodic Properties*, Cambridge University Press, Cambridge, 1994.

[81] I. Gutman, *The energy of a graph*, in: Ber. Math.-Stat. Sekt. Forschungszent. Graz 103, Graz, 1978.

[82] More precisely, the total π-electron energy can be calculated as the energy of an appropriate molecular graph. For connections between *Hückel molecular orbital theory* and graph spectral analysis, see R.B. Mallion, *Some chemical applications of the eigenvalues and eigenvectors of*

by others, has evolved into a significant, much studied mathematical object.[83] For a while it was thought that the maximal energy a graph with n vertices could have is $2(n-1)$, which incidentally is the energy of the complete graph K_n. This turned out to be false, but it triggered the search for high-energy graphs in certain classes of graphs.

Using the characterization of integral circulant graphs $\mathrm{ICG}(n, D)$ by the two parameters n and D, where n is the number of vertices of the graph and D is a set of divisors of n,[84] we abbreviate the energy of $\mathrm{ICG}(n, D)$ by setting $E(n, D) := E(\mathrm{ICG}(n, D))$. We ask for the *maximal energy* $E_{\max}(n)$, taken over all divisor sets D of n for any fixed n. Observe that, since all eigenvalues of $\mathrm{ICG}(n, D)$ are integral, the energy $E(n, D)$ is an integer as well. As a by-product, the authors' energy formula[85] revealed the arithmetical fact that $2(p-1) \mid E(p^s, D)$. More importantly, $E_{\max}(p^s)$ could be determined explicitly, and the divisor sets D maximizing the energy were found[86] by combinatorial arguments.

Due to the lack of a closed energy formula for $E(n, D)$, it seemed much more difficult to deal with $E_{\max}(n)$ for arbitrary n. A crucial obstacle is the problem that $E(n, D)$ reveals no signs of multiplicativity with respect to n. This deficiency was overcome by developing and using the concept of *multiplicative divisor sets*.[87] A divisor set D of n is called *multiplicative* if

$$D = \prod_{p \in \mathbb{P},\, p \mid n} D_p,$$

where D_p contains all powers of the prime $p \mid n$ which divide some element of D, and the product of sets $A_1, \ldots, A_k$ of numbers is defined by

$$\prod_{i=1}^{k} A_i = A_1 \cdot \ldots \cdot A_k = \{a_1 \cdot \ldots \cdot a_k : \ a_1 \in A_1, \ldots, a_k \in A_k\}.$$

certain finite, planar graphs, pp. 87–114 in: R.J. Wilson ed., *Appl. of combinatorics*, Shiva Math. Ser. 6, Shiva Publ., Nantwich, 1982.

[83] For mathematical surveys, see R.A. Brualdi, *Energy of a graph*, AIM Workshop Notes, 2006 and I. Gutman, *The energy of a graph: Old and new results*, pp. 196–211 in: A. Betten, A. Kohnert, R. Laue, A. Wassermann eds., *Algebraic Combinatorics and Applications*, Springer-Verlag, Berlin, 2001.

[84] As shown in Theorem 4.4.

[85] J.W. Sander and T. Sander, *The energy of integral circulant graphs with prime power order*, App. Anal. Discrete Math. **5** (2011), 22–36.

[86] J.W. Sander and T. Sander, *The exact maximal energy of integral circulant graphs with prime power order*, Contributions to Discrete Math. **8**(2) (2011), 19–40.

[87] T.A. Le and J.W. Sander, *Convolutions of Ramanujan sums and integral circulant graphs*, Int. J. of Number Theory **8**(7) (2012), 1777–1788.

For multiplicative divisor sets D of $n = p_1^{s_1} \cdots p_k^{s_k}$, we have the desired multiplicativity of the energy,[88] namely

$$E(n, D) = \prod_{i=1}^{k} E(p_i^{k_i}, D_{p_i}).$$

By restricting the divisor sets to those which are multiplicative, the following bound could be shown.[89]

Theorem 6.1 *Let n be a positive integer. Then*

$$E_{\max}(n) \leq n \sum_{d|n} \frac{\varphi(d)\tau(d)}{d} < \left(\tfrac{3}{4}\right)^{\omega(n)} n\,\tau(n)^2,$$

where φ denotes Euler's totient function, $\tau(n)$ the number of positive divisors of n, and $\omega(n)$ the number of distinct prime factors of n.

Multiplicative divisor sets are also useful when approaching the problem to determine the integral circulant graphs being Ramanujan graphs[90] at the same time. Again, the answer for $\mathrm{ICG}(p^s, D)$ could be given completely and explicitly.[91] In the general case $\mathrm{ICG}(n, D)$, a certain arithmetic feature, namely n having a comparatively dominating prime power factor, is crucial[92]:

Theorem 6.2 *Let $n \geq 3$ be an integer.*

(i) For even n, there is always a multiplicative divisor set D of n such that $\mathrm{ICG}(n, D)$ is a Ramanujan graph.

(ii) If n is odd and has a prime power factor $\geq \frac{n^{3/2}+n}{2(n-1)}$, then there is a multiplicative divisor set D of n such that $\mathrm{ICG}(n, D)$ is a Ramanujan graph.

(iii) If the largest prime power factor of some odd $n \geq 8259$ is smaller than $\frac{n^{3/2}+n}{2(n-1)}$, then there is no multiplicative divisor set D of n such that $\mathrm{ICG}(n, D)$ is a Ramanujan graph.

[88] Theorem 4.1 in footnote 87.

[89] T.A. Le and J.W. Sander, *Extremal energies of integral circulant graphs via multiplicativity*, Linear Alg. Appl. **437** (2012), 1408–1421.

[90] Cf. preceding section.

[91] T.A. Le and J.W. Sander, *Integral circulant Ramanujan graphs of prime power order*, Electronic J. Combinatorics **20** (2013), Research paper P35.

[92] J.W. Sander, *Integral circulant Ramanujan graphs via multiplicativity and ultrafriable integers*, Linear Algebra Appl. **477** (2015), 21–41.

The Leading Coefficients of Stern Polynomials

Andrzej Schinzel

In memory of Wolfgang Schwarz

Abstract The leading coefficient of the nth Stern polynomial defined by Klavžar et al. (Adv Appl Math 39:86–95, 2007) is expressed in terms of the binary expansion of n.

Keywords Binary expansion • Stern polynomial

2010 Mathematics subject classification: Primary 11B83; Secondary 11A63

We shall use the notion of Stern polynomials B_n, introduced by Klavžar, Milutinović and Petr [1], i.e. $B_1 = 1$, $B_{2n}(x) = xB_n(x)$, $B_{2n+1} = B_n + B_{n+1}$. Using the results of [2] and denoting by F_n the Fibonacci sequence we shall prove

Theorem 1 *If n has binary expansion*

$$n = \overset{a_1}{1}\,\overset{a_2}{0}\ldots\overset{a_k}{1} \quad (a_i > 0), \tag{1}$$

then the leading coefficient c_n of B_n is given by the formula

$$c_n = \prod_{i=1}^{I} N(A_i), \tag{2}$$

A. Schinzel (✉)
Institute of Mathematics, Polish Academy of Sciences, Śniadeckich 8, 00-656 Warsaw, Poland
e-mail: schinzel@impan.pl

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_25

where A_i are the blocks of 1's and 2's occurring in the sequence $a_2, \dots, a_k$. $N(A_i)$ are given by the formulae valid for integers l, m, where $l \geq 0$, $m \geq 0$ in (3) and (4); $l \geq 1$, $m \geq 1$ in (5) and (6),

$$N(\overset{l}{1}) = \begin{cases} 1 & \text{if } l \text{ is odd}, \\ \frac{l}{2} + 1 & \text{if } l \text{ is even}; \end{cases} \tag{3}$$

$$N(\overset{m}{2}) = F_{m+2}; \tag{4}$$

and

$$N(A, \overset{m}{2}, \overset{l}{1}) = \begin{cases} N(A, \overset{m-1}{2}) & \text{if } l \text{ is odd}, \\ \frac{l}{2} N(A, \overset{m-1}{2}) + N(A, \overset{m}{2}) & \text{if } l \text{ is even}; \end{cases} \tag{5}$$

$$N(A, \overset{l}{1}, \overset{m}{2}) = \begin{cases} F_{m+1} N(A, \overset{l}{1}) & \text{if } l \text{ is odd}, \\ F_{m+1} N(A, \overset{l}{1}) + F_m N(A, \overset{l-1}{1}) & \text{if } l \text{ is even}, \end{cases} \tag{6}$$

where A is a block of 1's and 2's either empty or ending with 1 or 2 in case (5) or (6), respectively.

Example If $n = 2^{a_2+a_3} + 2^{a_3} - 1$ (a_2, a_3 positive integers), then $c_n = 3$ for $n = 19$; $c_n = 2$ for $n = 5$, $2^{a_2+2} + 3$ ($a_2 > 2$), $2^{a_3+2} + 2^{a_3} - 1$ ($a_3 > 2$); $c_n = 1$, otherwise.

Corollary 1 *For n odd, B_n is monic if and only if (1) holds and the blocks of 1's and 2's occurring in the sequence $a_2, \dots, a_k$ have the form*

$$\overset{m_0}{2}\,\overset{l_1}{1}\,\overset{m_1}{2}\,\overset{l_2}{1} \dots \overset{l_h}{1}\,\overset{m_h}{2},$$

where l_i is odd, $0 \leq m_0 \leq 1$, $1 \leq m_i \leq 2$ ($0 < i < k$), $0 \leq m_k \leq 1$ ($k > 0$).

Theorem 2 *Let an integer $m > 0$ be given. For almost all n, in the sense of density, $c_n \equiv 0 \pmod m$.*

Corollary 2 *For almost all n, in the sense of density, B_n is not monic.*

Corollary 2 has been conjectured by M. Gawron (written communication).

For the proof of Theorem 1 we need a definition and five lemmas.

Definition 1 Let for a block A of 1's and 2's occurring in the sequence $a_2, \dots, a_k$ on the positions $a+1, \dots, b$ ($1 \leq a < b$) $N(A)$ be the number of integer sequences i_λ ($1 \leq \lambda \leq \Lambda$) such that

$$a < i_\lambda + 2 \leq b \quad (\lambda \leq \Lambda), \tag{7}$$

and for $\lambda < \Lambda$

$$i_{\lambda+1} \geq i_\lambda + 2 \tag{8}$$

and

$$\sum_{\lambda=1}^{\Lambda}(2 - a_{i_\lambda+2}) = \left\lfloor \frac{L_1 + 1}{2} \right\rfloor + \ldots + \left\lfloor \frac{L_J + 1}{2} \right\rfloor, \tag{9}$$

where $L_1, \ldots, L_J$ are the lengths of the blocks of 1's contained in A.

Lemma 1 (3) *holds.*

Proof In this case the condition (7) and Eq. (9) reduce to

$$a < i_\lambda + 2 \leq a + 1 + l \tag{10}$$

and

$$\Lambda = \left\lfloor \frac{l + 1}{2} \right\rfloor, \tag{11}$$

respectively. If l is odd, the only sequence satisfying (8) and (10)–(11) is

$$i_\lambda = a + 2\lambda - 3 \quad (1 \leq \lambda \leq \Lambda),$$

while if l is even the sequences satisfying (8) and (10)–(11) are

$$i_\lambda = a + 2\lambda - 3 \ (1 \leq \lambda < h), \quad i_\lambda = a + 2h - 2 \ (h \leq \lambda \leq \Lambda)$$

for $h = 1, \ldots, \frac{l}{2} + 1$. Thus (3) follows.

Lemma 2 *The number of integer sequences i_λ $(1 \leq \lambda \leq \Lambda)$, including the empty sequence, such that* (8) *holds and*

$$1 \leq i_\lambda \leq m \quad (m \geq 0,\ 1 \leq \lambda \leq \Lambda) \tag{12}$$

equals F_{m+2}.

Proof The lemma is true for $m = 0$, where only the empty sequence satisfies the conditions (8) and (12) and for $m = 1$, where there is only the empty sequence and the sequence $\{1\}$. Assume now that the lemma is true for all $m < n \geq 2$. Then every sequence satisfying

$$1 \leq i_\lambda \leq n \quad (1 \leq \lambda \leq \Lambda)$$

has either

$$i_\Lambda < n \tag{13}$$

or

$$i_\Lambda = n. \tag{14}$$

The number of sequences satisfying (8) and (13) is, by the inductive assumption, F_{n+1}, the number of sequences satisfying (8) and (14), since $i_{\lambda-1} \le n-2$ is, by the inductive assumption, F_n. Therefore, the total number is $F_n + F_{n+1} = F_{n+2}$, which completes the inductive proof.

Lemma 3 *Equation* (4) *holds.*

Proof In this case the condition (7) and Eq. (9) reduce to

$$a < i_\lambda + 2 \le a + m \quad (\lambda \le \Lambda)$$

and (4) follows from Lemma 2.

Lemma 4 *Equation* (5) *holds.*

Proof Let the length of the block A be α and the lengths of the blocks of 1's contained in A be $L_1, \dots, L_{J-1}$. Then the conditions (7) and Eq. (9) reduce to

$$a_{i_\lambda+2} \in A \quad (a < i_\lambda + 2 \le a + \alpha), \tag{15}$$

$$a_{i_\lambda+2} = 2 \quad (a + \alpha < i_\lambda + 2 \le a + \alpha + m), \tag{16}$$

$$a_{i_\lambda+2} = 1 \quad (a + \alpha + m < i_\lambda + 2 \le a + \alpha + m + l), \tag{17}$$

$$\sum_{a<i_\lambda+2\le a+\alpha} (2 - a_{i_\lambda+2}) = \left\lfloor \frac{L_1+1}{2} \right\rfloor + \ldots + \left\lfloor \frac{L_{J-1}+1}{2} \right\rfloor, \tag{18}$$

$$\sum_{a+\alpha+m<i_\lambda+2\le a+\alpha+m+l} (2 - a_{i_\lambda+2}) = \left\lfloor \frac{l+1}{2} \right\rfloor. \tag{19}$$

Let the least λ satisfying (17) be Λ_1. If l is odd, the only sequence i_λ ($\lambda \ge \Lambda_1$) satisfying (8) and (17), (19) is $i_\lambda = a + \alpha + m + 2(\lambda - \Lambda_1) - 1$ and thus, by (8), either $\Lambda_1 = 1$, or $i_{\Lambda_1-1} + 2 \le a + \alpha + m - 1$. Therefore,

$$N(A, \overset{m}{2}, \overset{l}{1}) = N(A, \overset{m-1}{2}). \tag{20}$$

If l is even and (8) holds, then either $\Lambda_1 = 1$, or

$$i_{\Lambda_1} = a + \alpha + m + 1 \ge i_{\Lambda_1-1} + 2, \tag{21}$$

or

$$i_{\Lambda_1} \geq a + \alpha + m. \tag{22}$$

The number of sequences i_λ $(\lambda \geq \Lambda_1)$ satisfying (8), (17), (19) and (21) is, by Lemma 1, $\frac{l}{2}$, on the other hand, the number of sequences i_λ $(\lambda < \Lambda_1)$ satisfying (8), (16) with $a+\alpha+m$ replaced by $a+\alpha+m-1$ and (18) is $N(A, \overset{m-1}{2})$. The number of sequences i_λ satisfying (8), (17), (19) and (22) is one, on the other hand, the number of sequences i_λ $(\lambda < \Lambda_1)$ satisfying (8), (16) and (18) is $N(A, \overset{m}{2})$. Therefore,

$$N(A, \overset{m}{2}, \overset{l}{1}) = \frac{l}{2} N(A, \overset{m-1}{2}) + N(A, \overset{m}{2}) \tag{23}$$

and (5) follows from (20) and (23).

Lemma 5 *Equation* (6) *holds.*

Proof Let the length of the block A be α and the lengths of the blocks of 1's contained in A be $L_1, \ldots, L_{J-1}$. Then the condition (7) and Eq. (9) reduce to (15), (18),

$$a_{i_\lambda+2} = 1 \quad (a+\alpha < i_\lambda + 2 \leq a+\alpha+l), \tag{24}$$

$$a_{i_\lambda+2} = 2 \quad (a+\alpha+l < i_\lambda + 2 \leq a+\alpha+l+m), \tag{25}$$

$$\sum_{a+\alpha<i_\lambda+2\leq a+\alpha+l} (2 - a_{i_\lambda+2}) = \left\lfloor \frac{l+1}{2} \right\rfloor. \tag{26}$$

Let the least λ satisfying (25) be Λ_2. If l is odd, then (8) and (26) imply that $\Lambda_2 > 1$,

$$i_{\Lambda_2-1} + 2 = a + \alpha + l \leq i_{\Lambda_2},$$

thus, by Lemma 3, the number of sequences i_λ $(\lambda \geq \Lambda_2)$ satisfying (8) and (25) is F_{m+1}. On the other hand, the number of sequences i_λ $(\lambda < \Lambda_2)$ is $N(A, \overset{l}{1})$, thus

$$N(A, \overset{l}{1}, \overset{m}{2}) = F_{m+1} N(A, \overset{l}{1}). \tag{27}$$

If l is even, then either

$$i_{\Lambda_2} \geq a + \alpha + l \tag{28}$$

or

$$i_{\Lambda_2} = a + \alpha + l - 1. \tag{29}$$

The number of sequences i_λ ($\lambda \geq \Lambda_2$) satisfying (8), (25) and (28) is, by Lemma 3, F_{m+1}. The number of sequences i_λ ($\lambda < \Lambda_2$) satisfying (8), (15), (18) and (24) is $N(A, \overset{l}{1})$. The equality (29) implies by (8) $i_{\Lambda_2+1} + 2 \geq a + \alpha + l + 3$, thus the number of sequences i_λ ($\lambda \geq \Lambda_2$) satisfying (8), (25) and (29) is, by Lemma 3, F_m. On the other hand, by (8), $i_{\Lambda_2-1} \leq a + \alpha + l - 1$, hence the number of sequences i_λ ($\lambda < \Lambda_2$) satisfying (8), (15), (18) and (29) is $N(A, \overset{l-1}{1})$. Therefore,

$$N(A, \overset{l}{1}, \overset{m}{2}) = F_{m+1} N(A, \overset{l}{1}) + F_m N(A, \overset{l-1}{1}) \tag{30}$$

and (6) follows from (27) and (30).

Proof (Proof of Theorem 1) By Theorems 1 and 2 and Lemmas 5 and 6 of [2], c_n is cardinality of the set S of integer sequences i_λ ($1 \leq \lambda \leq \mu$) such that

$$i_1 \geq 0, \quad (8) \text{ holds for all } \lambda < \mu \quad \text{and} \quad \sum_{\lambda=1}^{\mu} (2 - a_{i_\lambda+2}) = \left\lfloor \frac{l_1+1}{2} \right\rfloor + \ldots + \left\lfloor \frac{l_j+1}{2} \right\rfloor, \tag{31}$$

where $l_1, \ldots, l_j$ are lengths of blocks of 1's occurring in the sequence $a_2, \ldots, a_k$. Since the right-hand side is the maximum taken by the left-hand side for all sequences i_λ satisfying (31) we have for $i_\lambda \in S$, $a_{i_\lambda+2} \leq 2$ and

$$|S| = \prod_{i=1}^{I} N(A_i),$$

where A_i are blocks of 1's and 2's occurring in the sequence $a_2, \ldots, a_k$ and $N(A_i)$ are defined above. Theorem 1 follows now from Lemmas 1, 2, 4, 5.

Proof (Proof of Corollary 1) This follows at once from Theorem 1.

For the proof of Theorem 2 we need a definition and a lemma.

Definition 2 Let n satisfy (1). $J(n)$ is the number of the blocks $A_i(n)$ of 1's and 2's contained in $a_2, \ldots, a_k$.

Lemma 6 *For every fixed integer $l > 0$ the asymptotic density of odd n such that for a certain $i \leq J(n)$: $A_i(n) = \overset{2l}{1}$ is $1/2$.*

Proof Suppose that the lemma is false. Then there exists $\varepsilon > 0$ and a sequence x_ν such that $x_\nu \to \infty$ and the number of odd $n \leq x_\nu$ such that for all $i \leq J(n)$: $A_i(n) \neq \overset{2l}{1}$ is at least εx_ν. Put $s_\nu = \lceil \frac{\log x_\nu}{\log 2} \rceil$. We may assume that for all ν

$$s_{\nu+1} \geq s_\nu + 2l + 6. \tag{32}$$

The set S_ν of odd $a < 2^{s_\nu}$ such that for all $i \le J(a)$: $A_i(a) \ne \overset{2l}{1}$ satisfies

$$2^{s_\nu - 1} \ge |S_\nu| \ge \varepsilon 2^{s_\nu - 1}. \tag{33}$$

Let $T_\nu(x)$ be the set of all $n \le x$ such that

$$n \equiv 2^{s_\nu+2l+5} + 2^{s_\nu+2l+4} + 2^{s_\nu+2l+3} + 2^{s_\nu+2l+1} + 2^{s_\nu+2l-1} + \ldots + 2^{s_\nu+3} + a \pmod{2^{s_\nu+2l+6}}, \quad a \in S_\nu.$$

We have by (33) for all ν

$$|T_\nu(x)| > |S_\nu|\Big(\frac{x}{2^{s_\nu+2l+6}} - 1\Big) > \frac{\varepsilon x}{2^{2l+7}} - 2^{s_\nu - 1}. \tag{34}$$

Distinct sets $T_\nu(x)$ are disjoint. Indeed, if $\nu > \mu$ and

$$n \in T_\mu(x) \cap T_\nu(x)$$

then by (32) and (34)

$$\operatorname{res} n \bmod 2^{s_\nu} \equiv 2^{s_\mu+2l+5} + 2^{s_\mu+2l+4} + 2^{s_\mu+2l+3} + 2^{s_\mu+2l+1} + 2^{s_\mu+2l-1} + \ldots + 2^{s_\mu+3} + a \pmod{2^{s_\mu+2l+6}}, \quad a \in S_\mu,$$

thus the binary expansion of $\operatorname{res} n \bmod 2^{s_\nu}$ contains the segment

$$111\underbrace{01\ldots01}_{2l}000$$

contrary to the definition of S_ν. Put

$$E = \Big\lceil \frac{2^{2l+6}}{\varepsilon} \Big\rceil + 1, \quad x > \frac{2^{s_E+2l+7}}{\varepsilon}.$$

Then, since the number of odd $n \le x$ is at most $\frac{x+1}{2}$, we have by (34)

$$\frac{x+1}{2} \ge \Big|\bigcup_{\nu=1}^{E} T_\nu(x)\Big| = \sum_{\nu=1}^{E} |T_\nu(x)| > E\,\frac{\varepsilon x}{2^{2l+7}} - 2^{s_1-1} - \ldots - 2^{s_E-1} > \frac{x}{2} + \frac{\varepsilon x}{2^{s_E+7}} - 2^{s_E} + 1 \ge \frac{x}{2} + 1.$$

The obtained contradiction completes the proof.

Remark 1 One can prove similarly that for every block A of 1's and 2's with $0 < |A| < \infty$ the asymptotic density of n with $i \le J(n)$ and $A_i(n) = A$ is $1/2$.

Proof (Proof of Theorem 2) Taking in Lemma 6: $l = m-1$ ($m > 1$) we obtain from Theorem 1 that the asymptotic density of odd n such that $c_n \equiv 0 \pmod m$ is $1/2$. It follows that for every $\varepsilon > 0$ and for every positive integer k the number of odd $n \le \frac{x}{2^k}$ such that $c_n \equiv 0 \pmod m$ is $> (1-\varepsilon)x/2^{(k+1)}$ for $x > x_0(\varepsilon, k)$. Without loss of generality we may suppose that $x_0(\varepsilon, k)$ is increasing in k. Since $c_{2n} = c_n$, taking $k = \lfloor \frac{-\log \varepsilon}{\log 2} \rfloor$ we obtain that for $x > x_0(\varepsilon, k)$ the number of $n \le x$ such that $c_n \equiv 0 \pmod m$ is at least $(1 - \frac{1}{2^{k+1}} - \varepsilon)x > (1-2\varepsilon)x$, which proves the theorem.

Proof (Proof of Corollary 2) It suffices to take in Theorem 2: $m = 2$.

References

1. S. Klavžar, U. Milutinović, C. Petr, Stern polynomials. Adv. Appl. Math. **39**, 86–95 (2007)
2. A. Schinzel, Stern polynomials as numerators of continued fractions. Bull. Pol. Acad. Sci. **62**, 23–27 (2014)

The Non-existence of Universal Carmichael Numbers

Jan-Christoph Schlage-Puchta

To the memory of Wolfgang Schwarz

Abstract We show that universal elliptic Carmichael numbers do not exist, answering a question of Silverman. Moreover, we show that the probability that an integer n, which is not a prime power, is an elliptic Carmichael number for a random curve E with good reduction modulo n, is bounded above by $\mathcal{O}(\log^{-1} n)$. If we choose both n and E at random, the probability that n is E-Carmichael is bounded above by $\mathcal{O}(n^{-1/8+\epsilon})$.

Keywords Carmichael numbers • Elliptic curves • Pseudoprimes

2010 Mathematics subject classification: Primary 11G20; Secondary 11N25, 11Y11

1 Introduction and Results

Let E be an elliptic curve defined over $\mathbb{Q}$. Let $L(s, E) = \sum_{n\geq 1} \frac{a_n(E)}{n^s}$ be the L-series associated with E. If p is prime, then $|E(\mathbb{Z}/p\mathbb{Z})| = p - a_p(E) + 1$. Hence, if $a_n(E)$ is computable, checking whether $|E(\mathbb{Z}/n\mathbb{Z})| = n - a_n(E) + 1$ is a necessary criterion for n to be prime. Unfortunately the order of $E(\mathbb{Z}/n\mathbb{Z})$ is not directly accessible, so in practice one chooses a point P on the curve, and checks whether $(n - a_n(E) + 1)P = 0$. If this condition is satisfied for every $P \in E(\mathbb{Z}/n\mathbb{Z})$, but n is not a prime power, we say that n is a Carmichael number for the curve E.

Silverman [9] defined a universal elliptic Carmichael number to be an integer n, which has at least two different prime factors, but n is a Carmichael number for every elliptic curve E, which has good reduction modulo n, and asked whether

J.-C. Schlage-Puchta (✉)
Institut für Mathematik, Universität Rostock, 18051 Rostock, Germany
e-mail: jan-christoph.schlage-puchta@uni-rostock.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_26

universal elliptic Carmichael numbers exist. Here we show that such numbers do not exist. In fact, we can explicitly give parameters $a_p(E)$, which imply that n is not an elliptic Carmichael number for the curve E. While very explicit, this proof leaves the possibility that an integer n is elliptic Carmichael for most curves. Therefore we are also interested in the probability that an integer n is elliptic Carmichael for a random curve E. We prove the following:

Theorem 1.1 *Let n be an integer, which is not a prime power.*

1. *There exists a curve E with good reduction modulo n, such that n is not an elliptic Carmichael number for E.*
2. *As n tends to infinity, the probability that n is elliptic Carmichael for a random curve E is $\mathcal{O}(\log^{-1} n)$.*
3. *If $n \in [x, 2x]$ is chosen at random, and E is a random curve, then the probability that n is E-Carmichael is $\mathcal{O}(x^{-1/8+\epsilon})$.*

The implied constants are absolute and not too large, and come mostly from replacing terms of the form $\log\log n$ by $\log^{\epsilon} n$.

Note that Luca and Shparlinski [5] considered the dual question to part 2 of Theorem 1.1, i.e. if E is a fixed elliptic curve and n is chosen at random, then the number of E-Carmichael integers in $[x, 2x]$ is $\mathcal{O}(\frac{x}{\log\log x})$. The argument involved is quite different from our arguments, in particular, we do not have to consider twists $L(s, E, \chi)$ of the L-series associated with E.

Our notation follows the standard for analytic number theory. We denote by $\log_k$ the k-fold iterated logarithm, e.g. $\log_2 n = \log\log n$, by $\omega(n)$ the number of prime factors of n, $P^+(n)$ the largest prime factor of n. For an integer $n = \prod p_i^{e_i}$ we call $\gamma(n) = \prod p_i$ the squarefree kernel of n. For an integer n and a prime number p, denote by $v_p(n)$ the exponent of p in the prime decomposition of n, that is, the largest k such that $p^k | n$. For a group G we put $\exp(G)$, the exponent of G to be the least integer $n > 0$, such that $g^n = 1$ for all $g \in G$. We use $\ll$ as a synonym of $= \mathcal{O}(\dots)$, an index at a Landau symbol indicates that the implied constants depend on the index.

2 Preliminaries

In this section we collect results on the L-series of an elliptic curve and on multiplicative number theory.

Our first two statements are well known, and can, e.g., be found in [8].

Lemma 2.1 *The function $n \mapsto a_n$ is multiplicative, and satisfies $|a_n| \le 2^{\omega(n)}\sqrt{n}$. For each p there exists a complex number α_p of modulus $\sqrt{p}$, such that $a_{p^k} = \alpha^k + \overline{\alpha}^k$.*

Lemma 2.2 *The group $E(\mathbb{Z}/p\mathbb{Z})$ is a two-generated abelian group, and we have $\exp(E(\mathbb{Z}/p^k\mathbb{Z})) = p^{k-1}\exp(E(\mathbb{Z}/p\mathbb{Z}))$.*

Define the function $e : \mathbb{N} \to \mathbb{N}$ to be the multiplicative function satisfying $e(p^k) = p^{\lceil k/2 \rceil}$.

Lemma 2.3 *Let G be a two-generated abelian group. Then $e(|G|)|$ divides $\exp(G)$.*

Proof It follows from the classification of finitely generated abelian groups, that G can be written as $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ with $n_1|n_2$. Clearly $\exp(G) = n_2$, and we have that if $p^k|n_1n_2$, then $p^{\lceil k/2 \rceil}|n_2$. Hence our claim follows.

We will repeatedly use the following alternative definition of an elliptic Carmichael number, which is [9, Proposition 12].

Lemma 2.4 *An integer n is elliptic Carmichael for the curve E if and only if E has good reduction modulo n, and for each prime divisor p of n we have that $\exp(E(\mathbb{Z}/p^{v_p(n)}\mathbb{Z}))$ divides $a - a_n + 1$.*

Deuring [2] determined the number of curves modulo p having prescribed order.

Lemma 2.5 *Let p be a prime. Then the number of curves E modulo p with $|E(\mathbb{Z}/p\mathbb{Z})| = p - a_p + 1$ equals $H(4p - a_p^2)$, where $H(n)$ is the Kronecker class number, which can be computed as follows. Write $n = n'f^2$, where n' is squarefree and $(n', f) = 1$. Then*

$$H(n) = \frac{\sqrt{n}}{2\pi} L\left(1, \left(\frac{\cdot}{n'}\right)\right) \psi(f),$$

where ψ is the multiplicative function defined by

$$\psi(p^k) = \begin{cases} \frac{p-p^{-k}}{p-1}, & \text{if } \left(\frac{p}{n'}\right) = 0, \\ 1, & \text{if } \left(\frac{p}{n'}\right) = 1, \\ \frac{p+1-2p^{-k}}{p-1}, & \text{if } \left(\frac{p}{n'}\right) = -1. \end{cases}$$

The function ψ satisfies $1 \leq \psi(f) \ll \log_2^2 f$.

Using this result Lenstra [3] proved the following:

Lemma 2.6 *Let p be a prime, $S \subseteq [p - 2\sqrt{p}, p + 2\sqrt{p}]$ a set of integers. Then the probability that an elliptic curve E chosen at random satisfies $|E(\mathbb{Z}/p\mathbb{Z})| \in S$ is bounded above by $\mathcal{O}\left(\frac{|S|}{\sqrt{p}} \log p \log_2^2 p\right)$.*

If $|S|$ is not too small, we can do better.

Lemma 2.7 *For every fixed c we have that if p is a prime, and $S \subseteq [p - 2\sqrt{p}, p + 2\sqrt{p}]$ a set of integers satisfying $|S| > p^c$, then the probability P that an elliptic curve E chosen at random satisfies $|E(\mathbb{Z}/p\mathbb{Z})| \in S$ satisfies*

$$P \ll_c \frac{|S|}{\sqrt{p}} \log_2^3 p.$$

If $S \subseteq [p-(2-c)\sqrt{p}, p+(2-c)\sqrt{p}]$, *we also have*

$$P \gg_c \frac{|S|}{\sqrt{p}\log_2^2 p}$$

For the proof of Lemma 2.7 we need some zero density estimate. Since we are not interested in the implied constants, any result would do. We choose the following, because it is at the same time quite simple and very well known. We refer the reader to the Montgomery's book [6] for more detailed information.

Lemma 2.8 *For an integer* Q, *a real number* $T > 1$, *and a real number* $\sigma \geq 1/2$ *define* $N(\sigma, Q, T)$ *to be the number of pairs* (ρ, χ), *where* $\operatorname{Re}\rho \geq \sigma$, $|\operatorname{Im}\rho| \leq T$, χ *is a primitive character to a module* $q \leq Q$, *and* $L(\rho, \chi) = 0$. *Then we have* $N(\sigma, Q, T) \ll (Q^2T)^{\frac{12}{5}(1-\sigma)}\log^C(QT)$ *for some constant* C.

Proof (Proof of Lemma 2.7) It suffices to show that for all $q \leq Q = p + 2\sqrt{p}$ with at most p^c exceptions we have that

$$\log_2^{-1} q \ll_c L\left(1, \left(\frac{\cdot}{q}\right)\right) \ll \log_2 q. \tag{2.1}$$

In view of Lemma 2.8 it suffices to prove that (2.1) holds true under the assumption that $L\left(s, \left(\frac{\cdot}{q}\right)\right)$ has no roots in the domain $\operatorname{Re} s > 1 - c/8$, $|\operatorname{Im} s| \leq Q$. But under these assumptions (2.1) was essentially shown by Littlewood [4].

Lemma 2.9 *There exists an absolute constant* $c > 0$, *such that for all prime numbers* $p \in [x, x^2]$ *with at most one exception we have that the probability that* $a_p(E) = 1$ *holds true for a random curve* E *is* $\gg \frac{1}{\sqrt{p}\log p}$.

Proof This follows immediately from Lemma 2.5 and the fact that there is at most one modulus $q \in [x, x^2]$ for which a Siegel zero exists.

We shall also use the following consequence of Baker's bound for linear forms in logarithms:

Lemma 2.10 *Let* p *be a prime,* E *an elliptic curve. Then we have* $a_{p^k} \neq 1$ *for all* $k > 3 \cdot 10^{20}\log p(46 + \log_2 p)$.

Proof Define α_p as in Lemma 2.1. If $a_{p^k} = 1$, then $\alpha^k = 1 - \overline{\alpha}^k$, thus

$$0 < \Lambda = |k\log\alpha - k\log\overline{\alpha} - \log(-1)| \leq |\alpha|^{-k} = p^{-k/2}.$$

Here $\alpha, \overline{\alpha}$ are algebraic numbers of degree 2 and height $\leq p$, hence from the work of Baker and Wüstholz (confer, e.g., [1, Theorem 2.5]) we obtain

$$\Lambda \geq \exp(-96^{10}\log^2 p\max(1, \log k)).$$

Comparing these bounds we obtain

$$\frac{k\log p}{2} \le 96^{10}\log^2 p\max(1,\log k),$$
$$\frac{k}{2\log k} \le 96^{10}\log p,$$

which implies in particular $k \le 3\cdot 10^{20}\log p(46+\log_2 p)$. Hence our claim follows.

Lemma 2.11 *Let p be a prime, k an integer. Then there are $\le k$ integers $\alpha_1,\dots,\alpha_k$, such that for all a and all elliptic curves E we have that $a_{p^k}(E) = a$ implies $a_p(E) \in \{\alpha_1,\dots,\alpha_k\}$. Similarly there are k integers, such that for all a and all elliptic curves E we have that $a_{p^k}(E) \equiv a \pmod p$ implies $(a_p(E) \bmod p) \in \{\alpha_1,\dots,\alpha_k\}$.*

Proof Define α as in Lemma 2.1. There are two complex numbers with modulus $p^{k/2}$ and real part $a/2$. We may replace α by $\overline{\alpha}$, and may therefore assume that α^k is uniquely determined by a. Hence there are k possible choices for α realizing a, and our first claim follows. The second claim follows similarly by considering $\mathbb{F}_{p^2}$ in place of $\mathbb{C}$.

Lemma 2.12 *The number of integers $n \in [x, x+\sqrt{x}]$, which satisfy $e(n) < \frac{n}{k}$ is $\mathcal{O}(\frac{\sqrt{x}}{k} + x^{1/3}\log^3 x)$.*

Proof Write $n = ab^2c^3$, where a contains all prime divisors p of n, such that $p^2 \nmid n$, c contains all prime divisors of n, which divide n with an odd exponent ≥ 3, and $b = \sqrt{n/ac^3}$. We have $e(n) = n/bc$, hence the number of integers $n \in [x, x+\sqrt{x}]$ satisfying $e(n) < \frac{n}{k}$ equals

$$\sum_{bc>k}\left[\frac{x+\sqrt{x}}{b^2c^3}\right] - \left[\frac{x}{b^2c^3}\right] = \sum_{\substack{bc>k\\ b^2c^3<M}}\frac{\sqrt{x}}{b^2c^3} + \mathcal{O}(M^{1/2})$$
$$+ \mathcal{O}(\#\{n\in[x,x+\sqrt{x}] : \exists b,c : bc>k, b^2c^3>M, b^2c^3|n\}),$$

where M is a parameter to be chosen later. The first sum is $\mathcal{O}(\frac{\sqrt{x}}{k})$. To estimate the set in the second error term consider all integers $n \in [x, x+\sqrt{x}]$, which can be written as $n = ab^2c^3$, where $b^2c^3 > \sqrt{x}$, and $a \in [A, 2A]$, $b \in [B, 2B]$, $c \in [C, 2C]$. Clearly the whole range can be covered by $\mathcal{O}(\log^3 x)$ such intervals, hence, it suffices to estimate the maximum of the number of such n over all A, B, C with $2^5B^2C^3 > \sqrt{x}$. If two of the three integers a, b, c are determined, and $M > \sqrt{x}$, then there is at most one choice of the third such that $ab^2c^3 \in [x, x+\sqrt{x}]$, thus we obtain that the last error term is

$$\ll \log^3 x\max\{\min(AB, AC, BC) : AB^2C^3 \le x, B^2C^3 \ge M\}.$$

It is easy to see that the maximum is attained for $AB^2C^3 = x$, hence the second factor becomes

$$\max\{\min(xB/M, xC/M, BC) : B^2C^3 \geq M\}.$$

The function is non-decreasing in both B and C, hence, we may assume that $B^2C^3 = M$, and we obtain that the last quantity is

$$\max\{\min(x/(BC^3), x/(B^2C^2), BC) : B^2C^3 = M\} \ll x^{1/3},$$

since we can neglect the first term in the min and the side condition. Hence our claim follows.

3 Integers with Special Multiplicative Structure in Short Intervals

In this section we estimate the number of integers n in an interval of the form $[x, x + c\sqrt{x}]$, which satisfy certain constraints concerning their prime factorization.

Lemma 3.1 *Let $\mathcal{P}$ be a set of prime numbers, and let x be a sufficiently large real number. Then the number N of integers n in the interval $[x, x + \sqrt{x}]$ which can be written as dt, where $d < x^{2/3}$ and t contains only prime factors from the set $\mathcal{P}$ satisfies*

$$N \ll |\mathcal{P}| + \frac{\sqrt{x}\log|\mathcal{P}|}{\log x}.$$

If $|\mathcal{P}| < \frac{\log x}{4\log_2 x}$, then $N \ll |\mathcal{P}|$.

Proof Let $\mathcal{N} \subseteq [x, x + \sqrt{x}]$ be the set of integers which contain only prime factors from $\mathcal{P}$. We have

$$\prod_{n\in\mathcal{N}} n \leq x^{2|\mathcal{N}|/3} \prod_{p\in\mathcal{P}} \prod_{n\in\mathcal{N}} p^{v_p(n)}.$$

For a prime number $p \in \mathcal{P}$ the highest power of p dividing an element of $[x, x + \sqrt{x}]$ is $\leq x + \sqrt{x}$. Subtracting this element from all other elements of $\mathcal{N}$ we see that

$$\begin{aligned}\sum_{n\in\mathcal{N}} v_p(n) &\leq \frac{\log(x+\sqrt{x})}{\log p} + \sum_{k\geq 1} k \min\left(N, \left[\frac{\sqrt{x}}{p^k}\right]\right)\\ &\leq \frac{\log(x+\sqrt{x})}{\log p} + 4\min\left(N, \frac{\sqrt{x}}{p}\right)\end{aligned}$$

On the other hand, we have $\prod_{n\in\mathcal{N}} n \geq x^N$. If we compare these bounds we obtain

$$N|\log x^{1/3} \leq |\mathcal{P}|\log(x+\sqrt{x}) + N\sum_{\substack{p\in\mathcal{P}\\ p<\sqrt{x}/N}} \log p + \sqrt{x}\sum_{\substack{p\in\mathcal{P}\\ p>\sqrt{x}/N}} \frac{\log p}{p}$$

$$\leq 2|\mathcal{P}|\log x + (1+o(1))N\log\frac{\sqrt{x}}{N} + (1+o(1))\sqrt{x}\log|\mathcal{P}|$$

If $N > \frac{\sqrt{x}}{\log x}$, the first claim holds true anyway. Otherwise we obtain

$$N \leq 6|\mathcal{P}| + 2N\frac{\log_2 x}{\log x} + 3\frac{\sqrt{x}\log|\mathcal{P}|}{\log x},$$

and the first claim holds true again. If $|\mathcal{P}| < \frac{\log_2 x}{4\log x}$, we estimate $\sum_{p\in\mathcal{P}}\log p$ using the prime number theorem to be $\leq (\frac{1}{4}+o(1))\log x$. Hence

$$\frac{1}{3}N\log x \leq 2|\mathcal{P}|\log x + \frac{1}{4}N\log x,$$

which implies $N \leq 24|\mathcal{P}|$.

Next we prove the following:

Lemma 3.2 *There exists some $c > 0$, such that for x sufficiently large there are at least $c\sqrt{x}$ integers $n \in [x, x+0.1\sqrt{x}]$ which satisfy $P^+(n) > x^{1/2+c}$.*

Note that the question of finding integers with a large prime factor in a short interval has been studied since the work of Ramachandra [7], who proved that there is some $c > 0$ such that $[x, x+x^{1/2-c}]$ contains an integer divisible by a prime factor $> x^{1/2+1/13}$, however, for the present application we need that such integers not only exist but in fact are quite frequent. Still, although we could not find this result in the literature, the methods we use here are not new, and we will therefore be quite brief. The proof relies on the following two results:

Lemma 3.3 (Vaughan's Identity) *For integers U, V, n with $U < n$ we have*

$$\Lambda(n) = -\sum_{\substack{mdr=n\\ m\leq U\\ d\leq V}} \Lambda(m)\mu(d) + \sum_{\substack{hd=n\\ d\leq V}} \mu(d)\log h - \sum_{\substack{mk=n\\ m>U\\ k>1}} \Lambda(m)\left(\sum_{\substack{d|k\\ d\leq V}} \mu(d)\right)$$

The following follows from Weyl's estimates:

Lemma 3.4 *There is some $\alpha < 1$, such that for $N < x^{2/3}$ we have $\sum_{N\leq n<2N} e^{2\pi i x/n} \ll N^{\alpha}$*

Proof (Proof of Lemma 3.2) We estimate the number of integers in the interval $[x, x+0.1\sqrt{x}]$, which have a prime factor $\geq N$ by computing the sum

$$\begin{aligned}
&\sum_{n\geq N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right)\\
&=\sum_{n\leq x+0.1\sqrt{x}} \Lambda(n)\left[\frac{x+0.1\sqrt{x}}{n}\right]-\sum_{n\leq x+0.1\sqrt{x}} \Lambda(n)\left[\frac{x}{n}\right]\\
&\qquad -\sum_{n\leq N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right)\\
&=\log[x+0.1\sqrt{x}]!-\log[x]!-\sum_{n\leq N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right)\\
&=0.1\sqrt{x}\log x+\mathcal{O}(\log x)-\sum_{n\leq N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right).
\end{aligned}$$

Let $B(t)=t-[t]-\frac{1}{2}$ be the saw tooth function. Then we have

$$\begin{aligned}
&\sum_{N\leq n<2N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right)\\
&=0.1\sqrt{x}\sum_{N\leq n<2N}\frac{\Lambda(n)}{n}+\mathcal{O}\left(\sum_{N\leq n<2N}\Lambda(n)B\left(\frac{x}{n}\right)\right)\\
&\qquad +\mathcal{O}\left(\sum_{N\leq n<2N}\Lambda(n)B\left(\frac{x+0.1\sqrt{x}}{n}\right)\right)\\
&=\left(\frac{\log 2}{10}+o(1)\right)\sqrt{x}+\mathcal{O}\left(\sum_{N\leq n<2N}\Lambda(n)B\left(\frac{x}{n}\right)\right)\\
&\qquad +\mathcal{O}\left(\sum_{N\leq n<2N}\Lambda(n)B\left(\frac{x+0.1\sqrt{x}}{n}\right)\right)
\end{aligned}$$

Approximating B by a trigonometric polynomial and applying Lemmas 3.3 and 3.4 we see that for $N<x^{2/3}$ the error terms are $\ll N^{\alpha}$ for some $\alpha<1$. Putting these estimates together we obtain

$$\sum_{n\geq N} \Lambda(n)\left(\left[\frac{x+0.1\sqrt{x}}{n}\right]-\left[\frac{x}{n}\right]\right)=0.1\sqrt{x}\log x-0.1\sqrt{x}\log N+\mathcal{O}(N^{\alpha}).$$

Hence, if $N < cx^{1/(2\alpha)}$, and c is sufficiently small, the left-hand side of the last equation is $\geq 0.05\sqrt{x}\log x$, and our claim follows.

4 Proof of Theorem 1.1: The Non-existence of Universal Carmichael Numbers

In this section we prove the first part of Theorem 1.1. We begin with the case that n is not squarefree.

Lemma 4.1 *A universal elliptic Carmichael number is squarefree.*

Proof Let q be a prime number such that $q^2|n$, and let E be a curve such that $a_q = 0$. Then the algebraic number α defined in Lemma 2.1 equals $\sqrt{-p}$. Hence we obtain

$$a_{q^{\nu_q(n)}} = 2\mathrm{Re}\,(-p)^{\nu_q(n)/2} = \begin{cases} 0, & \nu_q(n) \equiv 1 \pmod 2, \\ \pm 2p^{\nu_q(n)/2}, & \nu_q(n) \equiv 0 \pmod 2. \end{cases}$$

By multiplicativity we conclude that $q|a_n$. Since $q|n$, we obtain that $n - a_n + 1$ is not divisible by q. But since $q^2|n$ we have that $q|\exp(E(\mathbb{Z}/q^{\nu_q(n)}\mathbb{Z}))$, hence, from Lemma 2.4 we see that n is not an elliptic Carmichael number for E.

Next we consider the case that n is squarefree.

Lemma 4.2 *Let n be a squarefree integer which has two different prime factors p, q, and let E be an elliptic curve which satisfies $a_p(E) = 1$, $a_q(E) = 0$. Then n is not elliptic Carmichael for the curve E.*

Proof From $a_q(E) = 0$ and multiplicativity we obtain $a_n = 0$. On the other hand, $a_p = 1$ implies that $\exp(E(\mathbb{Z}/p\mathbb{Z})) = p$, hence if n is elliptic Carmichael for E, then p divides both n and $n - a_n + 1 = n + 1$, which is impossible.

Clearly the case $a_p = 0$ is quite special. If n is not the power of a single prime, we can give examples of elliptic curves for which n is not E-Carmichael which are not supersingular for any prime divisor of n, however, for the prime power case we did not find such examples. Unless n has a lot of very small prime divisors, the probability for the event $a_n = 0$ is very small, which might leave the impression that being E-Carmichael is not a rare event. This impression was the main motivation for the remaining parts of Theorem 1.1.

5 Proof of Theorem 1.1: The Probability for n Fixed

The proof of the second part of Theorem 1.1 follows a bootstrap strategy. Our aim is to show that a potential counterexample has to be divisible by many small prime numbers to the first power. To do so we show that if n is a counterexample, then n

is not divisible by large primes, and by only few medium sized primes, and that $\frac{n}{\gamma(n)}$ is small. We shall begin with rather weak results in this direction, and then use the results on large prime divisors to strengthen the results on $\gamma(n)$, and vice versa.

Lemma 5.1 *Let n be an integer satisfying $\gamma(n) \le 2^{-\omega(n)}\sqrt{n}$. Then the probability that n is an elliptic Carmichael number for a random curve E is $\mathcal{O}(e^{-c\frac{\log^{1/3} n}{\log_2 n}})$ for some $c > 0$.*

Proof If E is a curve, for which n is an elliptic Carmichael number, then we have that $\exp(E(\mathbb{Z}/n\mathbb{Z}))$ divides $n - a_n + 1$. From Lemma 2.2 we see that $\frac{n}{\gamma(n)}$ divides $\exp(E(\mathbb{Z}/n\mathbb{Z}))$, hence $\frac{n}{\gamma(n)} | n - a_n + 1$. Clearly $\frac{n}{\gamma(n)} | n$, and we have $|a_n| \le 2^{\omega(n)}\sqrt{n}$, thus our assumptions imply $a_n = 1$. By multiplicativity this implies $a_{p^{\nu_p(n)}} = \pm 1$ for all prime divisors p of n.

From Lemma 2.10 we find that $\nu_p(n) \ll \log p \log_2 p$ for all prime divisors p of n. From Lemmas 2.6 and 2.11 we see that the probability that $a_{p^{\nu_p(n)}} = \pm 1$ is $\ll \frac{\nu_p(n)\log p \log_2^2 p}{\sqrt{p}} \ll \frac{\log^2 p \log_2^3 p}{\sqrt{p}}$. Suppose that n has a prime divisor $p_0 > e^{\sqrt[3]{\log n}}$. Then the probability for $a_{p_0^{\nu_{p_0}(n)}} = \pm 1$ is $\ll e^{-\sqrt[3]{\log n}/2} \log n$, which is sufficiently small. If n has no prime divisor $\ge e^{\sqrt[3]{\log n}}$, then we have for each prime divisor p of n that

$$p^{\nu_p(n)} \le e^{\mathcal{O}(\log^2 p \log_2 p)} \le e^{\mathcal{O}(\log^{2/3} n \log_2 n)},$$

thus n has $\gg \frac{\log^{1/3} n}{\log_2 n}$ different prime divisors. For each of them with a bounded number of exceptions we have that the probability for the event $a_{p^{\nu_p(n)}} = \pm 1$ is $\le 1/2$, hence, the probability for the event that $a_{p^{\nu_p(n)}} = \pm 1$ for all prime divisors of n is $< e^{-c\frac{\log^{1/3} n}{\log_2 n}}$, and our claim follows.

Lemma 5.2 *There exists some $c > 0$, such that for every $\epsilon > 0$ there exists some n_0 such that all integers $n > n_0$ with $\gamma(n) < \frac{n}{\log^4 n}$ we have that the probability that n is an elliptic Carmichael number for random curve E is $\mathcal{O}(\log^{-1} n)$.*

Proof Assume first that n is divisible by a prime number p, such that $p^2 \nmid n$. If n is an elliptic Carmichael number for E, then $\exp(E(\mathbb{Z}/n\mathbb{Z}))$ is divisible by $n/\gamma(n)$, hence we have $a_n \equiv 1 \pmod{n/\gamma(n)}$. By multiplicativity this implies $a_p \equiv \pm 1 \pmod{n/\gamma(n)}$, that is, a_p takes on only $\mathcal{O}(1 + \frac{\sqrt{p}}{n/\gamma(n)})$ values. We conclude that the probability that n is elliptic Carmichael for a random curve is bounded above by

$$\mathcal{O}\Big(\frac{\log p(\log\log p)^2}{n/\gamma(n)} + \frac{\log p(\log\log p)^2}{\sqrt{p}}\Big) = \mathcal{O}\Big(\frac{\log^2 p}{\sqrt{p}}\Big).$$

Clearly the conditions $a_p \equiv \pm 1 \pmod{\frac{n}{\gamma(n)}}$ are independent for different primes p, hence we conclude that if the product of all primes $p|n$, such that $p^2 \nmid n$ supersedes $\log^2 n \log_2^4 n$, then the probability for n to be E-Carmichael is $\ll \frac{1}{\log n}$.

Next suppose that $p \geq 5$ is a prime, such that $p^2|n$. We have $\frac{n}{\gamma(n)} | \exp(E(\mathbb{Z}/n\mathbb{Z}))$, hence, if n is elliptic Carmichael for the curve E, then

$$\frac{n}{\gamma(n)} \left| n - a_{n/p^{v_p(n)}} a_{p^{v_p(n)}} + 1. \right.$$

Since $\frac{n}{\gamma(n)}|n$, and $\frac{n}{\gamma(n)} \geq p^{v_p(n)-1} \geq p^{v_p(n)/2}$, we conclude that $a_{p^{v_p(n)}}$ is determined in $\mathcal{O}(1)$ ways. This in turn implies that a_p is determined in $\mathcal{O}(v_p(n))$ ways, and we find that the probability that n is E-Carmichael for a random curve is bounded above by

$$\frac{v_p(n) \log p \log_2 p}{\sqrt{p}} \ll \frac{\log n \log p \log_2 p}{\sqrt{n}}.$$

Hence if $p > \log^4 n \log_2^4 n$, our claim follows as well.

In particular we find that if n has a prime divisor $p > C \log^4 n \log_2^4 n$, then n is E-Carmichael with probability $\mathcal{O}(\log^{-1} n)$, no matter whether $p^2|n$ or not.

Next suppose that n is divisible by 3 prime numbers p_1, p_2, p_3, such that $p_i > \frac{1}{10} \log n$, and $2 \leq v_{p_i}(n) \leq 4$. Put $Q = \prod_{i=1}^3 p_i^{v_{p_i}(n)}$. Then we have that a_Q is uniquely determined modulo $\frac{Q}{\gamma(Q)}$, and since $16\sqrt{Q} \ll \frac{Q}{\gamma(Q)}$, we have that a_Q is determined in $\mathcal{O}(1)$ ways. If a_Q is fixed, then $a_{p_1^{v_{p_1}(n)}}, a_{p_2^{v_{p_2}(n)}}, a_{p_3^{v_{p_3}(n)}}$ are three integers with product a_Q, thus the number of choices for this triple is bounded above by

$$\max_{m \leq Q} \tau_3(m) \ll e^{\mathcal{O}(\frac{\log Q}{\log_2 Q})} \ll e^{\mathcal{O}(\frac{\log_2 n}{\log_3 n})}.$$

We conclude that the number of choices for the triple $(a_{p_1}, a_{p_2}, a_{p_3})$ is $\ll \log^\epsilon n$. Each fixed triple can be reached with probability $\ll \frac{\log^\epsilon n}{\sqrt{P}}$. Hence the probability that n is E-Carmichael is bounded above by

$$\frac{\log^\epsilon n}{P} \ll \frac{1}{\log^{3/2-\epsilon} n},$$

and we are done.

We now bound $\gamma(n)$. We have

$$\begin{aligned} \gamma(n) &= \prod_{p|n} p \\ &= \prod_{\substack{p|n \\ p^2 \nmid n}} p \prod_{\substack{p|n \\ 2 \leq v_p(n) \leq 4}} p \prod_{\substack{p|n \\ v_p(n) \geq 5}} p \end{aligned}$$

$$\leq \log^{18} n \prod_{p<\frac{1}{10}\log n} p \prod_{p^5|n} p$$
$$\ll n^{3/10} \log^{18} n,$$

and we are in the range already covered by Lemma 5.1.

Lemma 5.3 *Suppose that n is divisible by a prime number $p > n^{0.7}$. Then the probability that n is elliptic Carmichael for a random elliptic curve is $\mathcal{O}(n^{-0.05})$.*

Proof Write $n = dp$. Then we have $e(p - a_p + 1)|n - a_n + 1$, that is, $e(p - a_p + 1)|dp - a_d a_p + 1$. Since $e(p - a_p + 1)$ divides $p - a_p + 1$, we obtain

$$e(p-a_p+1)|n-a_n+1-d(p-a_p+1) = (d-a_d)a_p-d+1 \leq 2(d+2\sqrt{d})\sqrt{p} \leq \frac{3n}{\sqrt{p}} \leq 3n^{0.65}.$$

If $n - a_n + 1 - d(p - a_p + 1) \neq 0$, we obtain that $e(p - a_p + 1) < pn^{-0.05}$, which happens with probability $\ll n^{-0.05}$ in view of Lemma 2.12. If this quantity vanishes, then the divisibility property becomes trivial. But then we have $a_p = \frac{d-1}{d-a_d}$, which has at most one solution. Hence the probability for the event that this quantity vanishes is $\mathcal{O}(\frac{\log p \log_2 p}{\sqrt{p}})$, which is even smaller.

The previous lemma will not be used directly, but together with Lemma 5.2 we obtain the following, which shall be used repeatedly.

Lemma 5.4 *Suppose that n has not two prime divisors p_1, p_2, which satisfy $p_i > 0.1 \log n$, and $p_i^2 \nmid n$. Then the probability that n is elliptic Carmichael for a random curve E is $\mathcal{O}(\log^{-1} n)$.*

Proof Let n be an integer. If $P^+(n) > n^{0.7}$ or $\frac{n}{\gamma(n)} > \log^4 n$, our claim follows from Lemma 5.3 or Lemma 5.2, respectively. Hence assume that n satisfies none of these statements. We claim that for n sufficiently large this already implies that n has two prime divisors as described in the lemma. To see this assume the contrary. Let p_1, p_2 be the two largest prime divisors of n such that $p_i^2 \nmid n$. We want to show that these divisors exist and satisfy $p_i > 0.1 \log n$. Suppose the contrary. Then we have

$$n \leq \prod_{p<0.1\log n} p \cdot P^+(n) \cdot \left(\frac{n}{\gamma(n)}\right)^2 \leq e^{(0.1+o(1))\log n} n^{0.7} \log^8 n < n^{0.9},$$

which gives a contradiction.

Lemma 5.5 *Let n be an integer, $p_1 < p_2$ be prime divisors of n such that $p_i^2 \nmid n$. Write $n = dp_1p_2$. Let E an elliptic curve such that n is elliptic Carmichael for E. then one of the following holds true:*

1. *a_{p_1} is uniquely determined by a_d, a_{p_2};*
2. *$e(p_2 - a_{p_2} + 1) < 4\sqrt{p_1}(p_2/p_1)^{1/6}$;*

3. Putting $t = (e(p_2 - a_{p_2} + 1), n + 1)$ *we have* $t | a_d a_{p_2}$ *and* $t > p_2^{1/3}$.

Proof If n is elliptic Carmichael for E, then

$$e(p_2 - a_{p_2} + 1) | n - a_n + 1 = n - a_d a_{p_1} a_{p_2} + 1.$$

Assume that a_d and a_{p_2} are given. Put $t = (e(p_2 - a_{p_2} + 1), n + 1)$. Then $t | a_d a_{p_2}$, and a_{p_1} is uniquely determined modulo $q = \frac{e(p_2 - a_{p_2} + 1)}{t}$. On the other hand, we have $|a_{p_1}| \leq 2\sqrt{p}$, hence, if $q > 4\sqrt{p_1}$, then we have that a_{p_1} is uniquely determined in terms of a_d, a_{p_2}. If $q < 4\sqrt{p_1}$, we have that $t > p_2^{1/3}$ or $e(p_2 - a_{p_2} + 1) < 4\sqrt{p_1}(p_2/p_1)^{1/6}$. Hence in any case one of the statements (1)–(3) has to be true.

Lemma 5.6 *Suppose that* n *has* L *different prime divisors* $\leq M^2$. *Then* n *is E-Carmichael with probability* $\mathcal{O}(\log^{-1} n)$.

Proof For $1 \leq \nu \leq M$ let a_ν be the number of prime divisors of n in the interval $[\nu^2, (\nu + 1)^2)$. If p is a prime divisor of n in $[\nu^2, (\nu + 1)^2)$, then by the lower bound contained in Lemma 2.6 we have with probability $\geq \frac{a_\nu - 1}{\nu \log \nu \log_2 \nu}$ that $(p - a_p + 1, n) \geq \nu$.

Lemma 5.7 *The probability that* n *is elliptic Carmichael for a random curve* E *and at the same time* $a_n(E) = 0$ *is* $\mathcal{O}(\log^{-1} n)$.

Proof Suppose that n has two prime divisors $p_1, p_2 > e^{\log^{2/3} n}$. Then we obtain $e(p_i - a_p + 1) | n + 1$, and by Lemma 3.1 the probability for this event is $\ll \frac{\log \omega(n+1)}{\log p_i} \leq \frac{\log_2 n}{\log^{2/3} n}$. Since these two events are independent, our claim follows in this case.

The same argument applies if n has $\geq \log_2 n$ prime divisors $\geq \log^C n$, where C is a sufficiently large constant.

Let $c > 0$ be a constant as in Lemma 3.2. Suppose that n has $\geq \log_2^2 n$ prime divisors which are $\geq \log^{2-c} n$. If $q > 4\sqrt{p}$ is a prime divisor of $p - a_p + 1$, then q does not divide any other number of the form $p - a + 1$, $|a| \leq 2\sqrt{p}$. By Lemma 3.2 we have that the probability for the event $P^+(p - a_p + 1) > p^{1/2+c}$ is bounded away from 0, together with the fact that n has at most $\log n$ different prime divisors we conclude that probability for the event that $P^+(p - a_p + 1) > p^{1/2+c}$ and $P^+(p - a_p + 1) \nmid n + 1$ is bounded away from 0. But in the latter case we either have $a_n \neq 0$ or that n is not E-Carmichael. Since these events are independent for different p, we see that in this case our claim holds true as well.

Now assume that all prime divisors of n are $\leq n^{0.7}$, at most one prime divisor is $\geq e^{\log^{2/3} n}$, and at most $\log_2 n$ prime divisors of n are $\geq \log^C n$. We then give a lower bound for the product m of all prime divisors $p < \log^C n$ of n, such that $p^2 \nmid n$. We have

$$m > \frac{n}{P^+(n) e^{\log^{2/3} n \log_2 n} (\log^C n)^{\log_2^3 n}} > n^{0.2},$$

hence, n has at least $0.1\frac{\log n}{\log_2 n}$ prime divisors $p < \log^{3/2} n$, such that $p^2 \nmid n$. It then follows from Lemma 2.9 that the probability for the event that there exists a prime divisor p of m such that $a_p = 1$ is

$$\geq 1 - \left(1 - \frac{c}{\log^{3/4} n \log_2 n \log_3 n}\right)^{0.1 \log n / \log_2 n} \geq 1 - e^{-c' \frac{\log^{1/4} n}{\log_2^2 n \log_3 n}} \geq 1 - \frac{1}{\log^{-1} n},$$

hence, we may assume that there exists some p with $a_p = 1$. But then $p - a_p + 1 = p|n + 1$, contradicting $p|n$, and the proof is complete.

Therefore it suffices to consider the probability that n is elliptic Carmichael and satisfies $a_n(E) \neq 0$.

Lemma 5.8 *There exists a constant C such that if n is an integer, which is divisible by $> \log_2 n$ prime numbers $p > \log^C n$, then the probability that n is elliptic Carmichael for a random curve E is $\mathcal{O}(\log^{-1} n)$.*

Proof Let $p_1, \dots, p_k$ be the prime divisors of n which satisfy $p_i \geq \log^C n$. We put the pair p_1, p_i into Lemma 5.5. We may assume that $C \geq 7$. The probability that (1) holds true is $\ll \frac{\log_2 p_1 \log_3^2 p_1}{\sqrt{p_1}} \ll \log^{-2} n$. Using Lemma 2.12 we see that the probability that p_i, $i \geq 2$ satisfies (2) is $\ll \frac{p_1^{1/3} \log p_2 \log_2^2 p_2}{p_2^{5/6}} + \frac{\log^4 p_2 \log_2^2 p_2}{p_2^{1/3}}$, which is also $\ll \log^{-2} n$. We see that the probability that (1) or (2) holds true for at least one index i is bounded above by $\frac{k}{\log^2 n} < \frac{1}{\log n}$.

Taking for $\mathcal{P}$ the set of prime divisors of $n+1$ in Lemma 3.1 and using Lemma 2.6 we see that the probability that p_i, $i \geq 2$ satisfies (3) is bounded above by

$$\frac{\log n}{\log_2 n} \frac{\log p_i \log_2 p_i}{\sqrt{p}} + \frac{\log_2 n}{\log p}.$$

If $p > \log^C n$, the first summand is negligible as soon as $C > 2$, while the second summand becomes $\leq e^{-1}$ provided that C is sufficiently large. Since the third condition of Lemma 5.5 depends only on the second prime, we see that these events are independent, and that the probability that each p_i satisfies (3) is $e^{-k} \leq \frac{1}{\log n}$.

Lemma 5.9 *Suppose that n has 5 prime divisors $p_1, \dots, p_4$, such that $p_1 > \log^4 n$, and $p_2, \dots, p_4 > e^{\sqrt{\log n}}$, or 3 prime divisors, such that $p_1 > \log^4 n$, and $p_2, p_3 > p^{0.01}$. Then the probability that n is elliptic Carmichael for a random curve E is $\ll \log^{-1} n$.*

Proof We argue as in the proof of the previous theorem. The probability that p_1 satisfies (1) or that p_i, $i \geq 2$ satisfies (2) is $\ll \log^{-1} n$. In the first case the probability that one specific p_i, $i \geq 2$ satisfies (3) is $\ll \frac{\log_2^4 n}{\sqrt{\log n}}$, while in the second case the probability that one specific p_i satisfies (3) is $\ll \frac{\log_2^4 n}{\log n}$. Since the probabilities for

different p_i are independent we see that in each case the probability for the event that n is elliptic Carmichael is $\ll \log^{-1} n$.

Lemma 5.10 *There exists a $c > 0$, such that the following holds true. Suppose that n has $\geq \log_2^3 n$ prime divisors p satisfying $p > \log^{2-c/2} n$. Then the probability that n is elliptic Carmichael for a random curve E is $\mathcal{O}(\log^{-1} n)$.*

Proof Let c be as in Lemma 3.2. We may assume that at least half of the prime divisors p of n, which satisfy $p > \log^{2-c/2} n$ also satisfies $p < \log^C n$, where C is as in Lemma 5.8, for otherwise we can apply the latter. Cut the interval $[\log^{2-c/2} n, \log^C n]$ into $\mathcal{O}(1)$ intervals of the form $[x, x^{1+c}]$. Then one of these intervals contains $\gg \log_2^3 n$ prime divisors of n, let $[x, x^{1+c}]$ be the largest one of them. In particular the number of prime divisors p of n with $p > x^{1+c}$ is $\mathcal{O}(\log_2^3 n)$. For each prime divisor p of n with $x < p < x^{1+c}$ we have that $p - a_p + 1$ has a prime divisor $q > p^{1/2+c} \geq x^{1/2+c}$ with probability $\gg \frac{1}{\log p \log_2^2 p} \gg \frac{1}{\log_2 n \log_3^2 n}$. The probability that this prime is also a prime divisor of $n+1$ is $\ll \log^{-c/3} n$, hence with probability $\geq 1 - (1 - \frac{C}{\log_2 n \log_3^2 n})^{c \log_2^3 n} \geq 1 - \mathcal{O}(\log^{-1} n)$ we have that there exists a prime $q > x^{1/2+c}$, which divides some $p - a_p + 1$ for some $p|n$, but $q \nmid n + 1$.

But then n is Carmichael with probability $\leq \frac{1}{q} \ll \frac{1}{\log n}$, and our claim follows.

We can now prove part 2 of Theorem 1.1. It follows from Lemmas 5.3, 5.8 and 5.9, that either our claim is true, or n has $\geq c \frac{\log n}{\log \log n}$ prime divisors in the interval $[c \log n, \log^{2-c} n]$. In the latter case there exists some interval $[y, y + y^{1/2}]$, $c \log n < y < \log^{2-c} n$, which contains $\geq \log^{1/2+c/3} n$ prime divisors of n. For each of these prime divisors the probability that $p - a_p + 1$ happens to be another prime divisor of n is $> \log^{-1/2+c/4} n$, and for different prime divisors these probabilities are independent. We can therefore apply Černov's inequality to find that with probability $> 1 - \log^{-1} n$ we have that there are $> \log^{c/2} n$ prime divisors $p_1, \ldots, p_k$ of n, such that for each p_i there exists some q_i, such that $p_i = q_i - a_{q_i} + 1$. In particular for each of these prime divisors p_i we have that $p_i | n - a_n + 1$, since p_i also divides n, we obtain $a_n \equiv 1 \pmod{\prod p_i}$. Pick three prime divisors $c \log n < r_1, r_2, r_3 < \log^2 n$ of n, which are not among the q_i, and such that $r_i^2 \nmid n$. If such prime numbers do not exist, we discard some of the q_i in such a way, that the remainder still contains $\log^{c/2} n$ primes.

If n is E-Carmichael, then $a_{r_1 r_2 r_3}$ is uniquely determined modulo $\prod p_i > 8 \log^3 n$, hence this product is in fact uniquely determined. If $a_{r_1 r_2 r_3} = 0$, then our claim follows from Lemma 5.7. Otherwise if $a_{r_1 r_2 r_3}$ is given, then $(a_{r_1}, a_{r_2}, a_{r_3})$ can be chosen in

$$\tau_3(a_{r_1 r_2 r_3}) \ll e^{c \frac{\log_2 n}{\log_3 n}}$$

ways, and for each possible choice is realized with probability $\ll \prod_{i=1}^{3} \frac{\log r_i \log_2 r_i}{\sqrt{r_i}}$. Hence the probability that n is E-Carmichael is bounded above by

$$\prod_{i=1}^{3} \frac{\log r_i \log_2 r_i}{\sqrt{r_i}} e^{c\frac{\log_2 n}{\log_3 n}} \ll \log^{-3/2+\epsilon} n,$$

and the proof is complete.

6 Proof of Theorem 1.1: The Probability for n and E Variable

The proof of the third part of Theorem 1.1 is similar to the proof of the second part, but a lot easier, since we can dispose of integers with strange multiplicative behaviour immediately.

Lemma 6.1 *Let $n \in [x, 2x]$ and E be chosen at random. Then the probability that $P^+(n) > y$ and that n is E-Carmichael is $\mathcal{O}(x^\epsilon y^{-1/2})$.*

Proof The probability that n is divisible by $P^+(n)^2$ is $\mathcal{O}(y^{-1})$, hence, we may neglect this case. Put $p = P^+(n)$. Then we obtain $p - a_p + 1 | n - a_n + 1$, subtracting $a_{n/p}(p - a_p + 1)$ from the right-hand side we obtain

$$p - a_p + 1 | n - pa_{n/p} - a_{n/p} + 1. \tag{6.1}$$

If the right-hand side is 0, then $n+1 = (p+1)a_{n/p}$. In particular $a_{n/p} \equiv 1 \pmod p$, thus either $a_{n/p} = 1$, or $p \le 2\sqrt{n/p}$. In the first case we have $n = p$, thus n is prime, and therefore not Carmichael. In the second case we obtain $n + 1 \le (p + 1)a_{n/p} \le 5\sqrt{n/p}$, hence $P^+(n) \le 25$. Since the number of integers $n \in [x, 2x]$ with $P^+(n)$ can be bounded by some power of $\log x$, we may neglect this case as well, and assume from now on that the right-hand side of (6.1) is non-zero.

If $n - pa_{n/p} - a_{n/p} + 1$ is a non-zero integer, then it has $\ll e^{c\frac{\log}{\log\log x}}$ divisors. Hence for p and $a_{n/p}$ fixed, we have that among all possible choices for a_p there are only x^ϵ satisfying (6.1). The probability for hitting one of these choices is $\ll p^{-1/2} \log p x^\epsilon \ll y^{-1/2} x^\epsilon$, hence our claim follows.

Lemma 6.2 *Fix a squarefree integer $d \le x$, which is not divisible by any prime number $< \log^3 x$. Pick an integer $n \in [x, 2x]$ and an elliptic curve E at random. Then the probability that $d|n$, $(d, n/d) = 1$, and that n is E-Carmichael is at most $\mathcal{O}(x^{-\frac{1}{8}+\epsilon} + x^\epsilon d^{-\frac{4}{3}})$.*

Proof Fix the curve E modulo d, and put $H = \exp(E(\mathbb{Z}/d\mathbb{Z}))$. Then we have $H | n - a_d a_{n/d} + 1$, thus $a_{n/d}$ is determined modulo $\frac{H}{(H, a_{n/d})}$. Since $(H, a_{n/d}) | n + 1$, we conclude that $a_{n/d}$ is determined modulo $\frac{H}{(H, n+1)}$. The probability for the event

$d|n$ and $(n+1,H) \geq \sqrt{H}$ is $\ll \frac{1}{\sqrt{Hd}} + \frac{1}{x}$, if $(n+1,H) < \sqrt{H}$, there are $\leq \sqrt{\frac{n}{dH}}$ choices for $a_{n/d}$, which could lead to Carmichael numbers.

We next show that the number of choices for a_{p^k}, $p^k \| \frac{n}{d}$, which leads to a specific $a_{n/d} \neq 0$ is $\ll x^{\epsilon}$. There are $\ll \log x$ prime factors of $a_{n/d}$, distributing them over the possible a_{p^k} can be done in at most

$$\binom{\Omega(a_{n/d}) + \omega(n/d)}{\omega(n/d)} \leq \left(\frac{C\log x + C\frac{\log x}{\log\log x}}{\frac{\log x}{\log\log x}} \right)^{C\frac{\log x}{\log\log x}} \ll \exp(C\frac{\log x \log\log\log x}{\log\log x}).$$

different ways.

Fixing the values a_{p^k}, the number of choices for a_p is at most k by Lemma 2.11, hence the number of possible choices for a_p, $p|n/d$ given a_{p^k} for all $p^k \| n/d$ is bounded above by $\max n_1 n_2 \cdots n_\ell$, where the maximum is taken over all positive integers satisfying $n_1 + \cdots + n_k = \Omega(n/d) \leq \frac{\log 2x}{\log 2}$, and $\ell = \omega(d) \ll \frac{\log x}{\log\log x}$. Clearly this maximum is bounded above by

$$\left(\frac{\log x}{\ell \log 2} \right)^{\ell} \ll \exp(C\frac{\log x \log\log\log x}{\log\log x}).$$

We conclude that for any n, d the probability that $H|n - a_d a_{n/d} + 1$ subject to the condition $a_{n/d} \neq 0$ and $(H, n+1) < \sqrt{H}$ is $\ll x^{\epsilon}(\frac{1}{\sqrt{H}} + \sqrt{\frac{d}{n}})$.

If $a_{n/d} = 0$, then $H|n+1$, which is impossible for $(H,d) > 1$, and happens with probability $\leq \frac{1}{Hd} + \frac{1}{x}$ otherwise. Summarizing we obtain that the probability for the event $d|n$, $H|n - a_d a_{n/d} + 1$ is $\ll x^{\epsilon}(\frac{1}{d\sqrt{H}} + \frac{1}{x})$. If we choose $n \in [x, 2x]$ at random, the probability for the event that $d|n$, $H|n - a_d a_{n/d} + 1$, and $(H, n+1) < \sqrt{H}$ is $\ll x^{\epsilon}(\frac{1}{d\sqrt{H}} + \frac{1}{\sqrt{dx}})$.

It remains to show that with high probability we have that H is large. Write $d = p_1 \cdots p_k$, and put $H_i = |E(\mathbb{Z}/p_1 \cdots p_i \mathbb{Z})|$. Call a prime p_i bad, if $(H_{i-1}, |E(\mathbb{Z}/p_i\mathbb{Z})|) > p_i^{1/3}$. It follows from Lemma 3.1 that either $H_{i-1} > x^{1/4}$, or the probability that p_i is bad is bounded by $\mathcal{O}(\frac{\log x}{p_i \log\log x}) = \mathcal{O}(p_i^{-2/3})$. Hence either $H > x^{1/4}$, or the probability that the product of the bad primes is $> y$ is bounded above by $x^{\epsilon} y^{-2/3}$. Hence with probability $\geq 1 - x^{\epsilon} y^{-2/3}$ we obtain $H > \min(x^{1/4}, (d/y)^{2/3})$. Splitting the interval for y dyadically we obtain that the probability for the event that n is Carmichael is bounded above by

$$x^{\epsilon} \max_{1 \leq y \leq d} y^{-2/3} \left(\frac{1}{d\sqrt{(d/y)^{2/3}}} + \frac{1}{dx^{1/8}} + \frac{1}{\sqrt{xd}} \right) \ll x^{\epsilon} \left(\frac{1}{dx^{1/8}} + \frac{1}{\sqrt{xd}} + \frac{1}{d^{4/3}} \right)$$

Denote by $\Psi(x,y)$ the number of integers $n \leq x$, such that $P^+(n) \leq y$. The following is a consequence of Rankin's trick, see [10, Theorem III.5.2].

Lemma 6.3 *We have* $\Psi(x, \log^3 x) = x^{2/3 + o(1)}$.

We can now prove the third part of Theorem 1.1. Consider first the set of integers n which contain a divisor $D_1 \le d \le D_2$, such that d is squarefree, coprime to n, and all prime divisors of d are larger than $\log^3 n$. Using Lemma 6.2 we obtain that the probability that n satisfies this condition and is E-Carmichael for a random curve E is bounded above by

$$x^\epsilon \sum_{D_1 \le d \le D_2} (d^{-1}x^{-1/8} + d^{-1/2}x^{-1/2} + d^{-4/3}) \ll x^\epsilon (x^{-1/8} + D_2^{1/2}x^{-1/2} + D_1^{-1/3}).$$

If n does not possess such a divisor, then either $P^+(n) > D_2$, or we have $\prod^*_{p|n} p^{\nu(p)} > n/D_1$, where the product is taken over all prime divisors p of n, which are $\le \log^3 n$ or satisfy $\nu_p(n) \ge 2$. In the first case we can apply Lemma 6.1 to find that the probability that n is E-Carmichael is $\ll x^\epsilon D_2^{-1/2}$. In the second case we can write $n = abc$, where $P^+(a) \le \log^3 x$, b is powerful, and $c < D_1$. Using Lemma 6.3 we see that for given c the number of possible choices for ab is $\ll (x/c)^{2/3+\epsilon}$. Summing over c we find that the number of possible choices for n is $x^{2/3+\epsilon}D_1^{1/3}$. Hence the probability that a random n satisfies this condition is $\ll (x/D_1)^{-1/3+\epsilon}$. Summing up we find that the probability that a random n is E-Carmichael for a random curve E is bounded above by

$$x^\epsilon (x^{-1/8} + D_2^{1/2}x^{-1/2} + D_1^{-1/3} + D_1^{1/3}x^{-1/3} + D_2^{-1/2}).$$

In a wide range of parameters, e.g. for $D_1 = x^{3/8}$, $D_2 = x^{3/4}$, we have that the first term dominates the other terms, hence we conclude that the probability that n is E-Carmichael for n and E chosen at random is $x^{-1/8+\epsilon}$.

Note that the numerical value of the exponent can probably be improved, actually, we have no idea what the real value should be. It could well be something like $-1 + \epsilon$, however, this would probably be hard to prove.

References

1. A. Baker, G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*. New Mathematical Monographs, vol. 9 (Cambridge University Press, Cambridge, 2007)
2. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. **14**, 197–272 (1941)
3. H.W. Lenstra, Factoring integers with elliptic curves. Ann. Math. **126**, 649–673 (1987)
4. J.E. Littlewood, On the class-number of the corpus $P(\sqrt{-k})$. Proc. Lond. Math. Soc. (1) **27**, 358–372 (1928)
5. F. Luca, I. Shparlinski, On the counting function of elliptic Carmichael numbers. Canad. Math. Bull. **57**, 105–112 (2014)
6. H.L. Montgomery, *Topics in Multiplicative Number Theory*. Lecture Notes in Mathematics, vol. 227 (Springer, New York, 1971)

7. K. Ramachandra, A note on numbers with a large prime factor. J. Lond. Math. Soc. (2) **1**, 303–306 (1969)
8. J.H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 106 (Springer, New York, 1986)
9. J.H. Silverman, Elliptic Carmichael numbers and elliptic Korselt criteria. Acta Arith. **155**, 233–246 (2012)
10. G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*. Cambridge Studies in Advanced Mathematics, vol. 46 (Cambridge University Press, Cambridge, 1995)

Arithmetic Properties of Blocks of Consecutive Integers

Tarlok N. Shorey and Rob Tijdeman

In grateful Memory of Wolfgang Schwarz

Abstract This paper provides a survey of results on the greatest prime factor, the number of distinct prime factors, the greatest squarefree factor and the greatest m-th powerfree part of a block of consecutive integers, both without any assumption and under assumption of the *abc*-conjecture. Finally we prove that the explicit *abc*-conjecture implies the Erdős–Woods conjecture for each $k \geq 3$.

Keywords Block of integers • Greatest prime factor • Greatest squarefree divisor • Number of prime factors • Powerfree part

2010 Mathematics subject classification: Primary 11A51; Secondary 11D41

1 Introduction

Arithmetic properties of blocks of integers play an important role in various number theoretic questions. Let n and k be integers with $n > k \geq 3$ and consider $N = n(n+1)\cdots(n+k-1)$. Lower bounds on the greatest prime factor and the number of distinct prime divisors of N are used in results on Diophantine equations of the

The authors "Tarlok N. Shorey and Rob Tijdeman" are grateful for the hospitality of the Max-Planck-Institute for Mathematics in Bonn, Germany. A basis of this paper was laid during a stay of the first author from May until July, 2014, and of the second author in July.

T.N. Shorey
Indian Institute of Technology, Powai, Mumbai 400 076, India
e-mail: shorey@math.iitb.ac.in

R. Tijdeman (✉)
Mathematical Institute, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands
e-mail: tijdeman@math.leidenuniv.nl

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_27

form $N = y^q$ where $y > 1, q > 1$ are integers (see, e.g., [17, 22, 35]) and on irreducibility of polynomials (see, e.g., [14, 15, 39]). It is a question of Erdős and Graham [13, p. 67], which disjoint blocks of positive integers each of length ≥ 4 have a perfect power as the product of their terms. The question was answered in the negative for more than two blocks by Ulas [45] and Bauer and Bennett [7]. See also [8, 28]. It happens for two blocks if and only if the squarefree parts of the products of the terms of both blocks are equal. Therefore estimates on the squarefree part of N restrict the range of possible solutions. An open conjecture of Erdős and Woods [12] states that there is a k such that there are no positive integers $n_1 < n_2$ such that the integers $n_1 + i$ and $n_2 + i$ have exactly the same prime divisors for $i = 0, 1, \ldots, k-1$. In results on this question the greatest squarefree divisor plays a crucial role.

In this paper we give a survey of results on these functions in the literature and add some new results. Notation is introduced in Sect. 2. In Sect. 3 we summarize results on the greatest prime factor of N, in Sect. 4 those on the number of distinct prime factors on N. Sect. 5 deals with the greatest squarefree divisor of N and Sect. 6 with the greatest m-th powerfree part of N. Sect. 7 contains results on the problem of Erdős and Woods.

The *abc*-conjecture provides good insight into the true behaviour of the considered functions. In Sect. 8 we mention the results which have been obtained under assumption of the *abc*-conjecture. In Sect. 9 we apply the explicit *abc*-conjecture to the Erdős–Woods conjecture. Finally we refer in Sect. 10 to generalizations in the literature of the results mentioned in this survey.

New in this paper are a lower bound for the greatest prime factor of N when n is very large compared to k, see Theorem 3.1, another approach to prove results on the greatest m-th powerfree part of N for given k under the *abc*-conjecture, a new estimate for the greatest prime factor of N for general n and k under the *abc*-conjecture, Theorem 8.2, and the proof that the explicit *abc*-conjecture implies the Erdős–Woods conjecture for each $k \geq 3$, Theorem 9.1.

2 Notation

We write $P(x)$ for the greatest prime factor of the integer x, $\omega(x)$ for the number of distinct prime factors of x, $R(x)$ for the greatest squarefree factor (the 'radical') of x and $Q_m(x)$ for the greatest m-th powerfree part of x. We put $P(1) = 1, \omega(1) = 0$, $R(1) = Q_m(1) = 1$. Let

$$N = n(n+1)\cdots(n+k-1) \tag{2.1}$$

and

$$P(n,k) = P(N), \omega(n,k) = \omega(N), R(n,k) = R(N), Q_m(n,k) = Q_m(N). \tag{2.2}$$

We write $\exp_2 x$ for $\exp\exp x$, $\log_2 x$ for $\log\log x$, and so on. We use the Vinogradov symbols $\ll$ and $\gg$ where the attached parameters indicate on which the constants involved depend. In a similar way we use the Landau symbols $O(\cdot)$ and $o(\cdot)$.

3 The Greatest Prime Factor

Here we only formulate the best available results. For the history and more details we refer to [23] and Sect. 1.1 of [38].

3.1 Complete Results

Sylvester proved in 1892 that a product of k consecutive positive integers greater than k is divisible by a prime exceeding k. This has been refined by Laishram and Shorey [23] to

$$P(n,k) > 1.8k \text{ for } n > k$$

unless $(n,k) \in \{(8,3),(6,4),(7,4),(15,13),(16,13),(4,3),(5,4),(6,5),(9,8),(12,11),(14,13),(15,14),(19,18),(64,63)\}$, to

$$P(n,k) > 1.97k \text{ for } n > k + 13$$

and to

$$P(n,k) > 2k \text{ for } n > \max(k + 13, 279k/262).$$

Further they calculated all the exceptions to the inequality $P(n,k) > 1.95k$ with $n > k$, but this list is too long to be reproduced here. They noted that the restrictions on n,k are necessary. For example, $P(279,262) \le 2 \times 262$.

Nair and Shorey [30] proved that

$$P(n,k) > 4.42k \text{ for } n > 4k$$

and that

$$P(n,k) > 4.5k \text{ for } n > 4k \text{ and } k \neq 82, 83.$$

This implies that for $n > 100$

$$P(n,k) > 4.42k$$

whenever $n, n+1, \ldots, n+k-1$ are all composite.

3.2 Asymptotic Results

If $n \le k^{1.9}$ and n is sufficiently large, it follows from the results on the difference between consecutive primes (see, e.g., [3]) that there is a prime in $[n, n+k-1]$. Hence $P(n,k) \ge n$ whenever n is sufficiently large and $n < k^{1.9}$

For $n < k^{2-\varepsilon}$ with $0 < \varepsilon \le 0.1$ the best result up to now is due to Jia and Liu [20], viz.

$$P(n,k) \gg_\varepsilon k^{\frac{25}{13}-\varepsilon}.$$

Harman [19, Chap. 6] proved

$$P(k^2,k) \gg k^{1.48}.$$

For $k^2 < n \le \exp(c_1(\log k)^{3/2}/(\log_2 k)^{1/2})$ for suitable c_1 the best available result is due to Sander [33], viz.

$$P(n,k) \gg k^{1+c_2(\log k/\log n)^2}$$

for some positive constant c_2.

For $\exp(c_1(\log k)^{3/2}/(\log_2 k)^{1/2}) < n \le \exp_2\left((\log_2 k)^3/(\log_3 k)^2\right)$ the best available bound is due to Shorey [34], viz.

$$P(n,k) \gg k \log k \frac{\log_2 k}{\log_3 k}. \tag{3.1}$$

For $\exp_2\left((\log_2 k)^3/\log_3 k)^2\right) < n \le \exp_2(\log^2 k/\log_2 k)$ the best available bound is due to Ramachandra [31], viz.

$$P(n,k) \gg k \log k \left(\frac{\log_2 n}{\log_2 k}\right)^{1/2}. \tag{3.2}$$

For $n > \exp_2(\log^2 k/\log_2 k)$ this is superseded by a result of the authors [36]:

$$P(n,k) \gg k \log_2 n.$$

Combining the above results we see that (3.1) is valid for $n > k^{3/2}$.

According to Langevin [26] the constant involved in (3.2) can be arbitrarily close to 1 by letting n tend to ∞. Here we shall derive the following sharpening by using an improved linear form estimate due to Matveev [29]. The proof is an extension of [42, Sect. 10] where the case $k = 2$ was treated.

Theorem 3.1 *For $k \geq 2$, $n > \exp_2 k$ and n sufficiently large we have*

$$P(n,k) \gg k \log_2 n \frac{\log_3 n}{\log_4 n}.$$

Proof Suppose $N = p_1^{k_1} \cdots p_s^{k_s}$ with distinct primes $p_1, \ldots, p_s$ and positive integers $k_1, \ldots, k_s$. Let $P = P(n,k) = \max_{i=1,\ldots,s} p_i$. Suppose $\omega(n+h) = \min_{i=0,\ldots,k-1} \omega(n+i)$. Let $n+h = p_1^{h_1} \cdots p_s^{h_s}$ and $n+j = p_1^{j_1} \cdots p_s^{j_s}$ for any $j \neq h, j \in \{0, \ldots, k-1\}$. Then

$$0 < \left| \frac{p_1^{j_1} \cdots p_s^{j_s}}{p_1^{h_1} \cdots p_s^{h_s}} - 1 \right| < \frac{k}{n}. \tag{3.3}$$

Set $s_i = \omega(n+i)$ for all i. Note that for each j with $0 \leq j < k$ at most $\omega(n+j) + \omega(n+h) \leq 2s_j$ primes have nonzero exponents. We apply the following special case of a linear form estimate.

Lemma 3.2 (Matveev [29]) *Let $p_1, \ldots, p_s$ be primes. Put $\Omega = \prod_{j=1}^{s} \log p_j$. Then there exists an absolute constant c_3 such that the inequalities*

$$0 < |p_1^{b_1} \cdots p_s^{b_s} - 1| < \exp(-e^{c_3 s} \Omega \log B)$$

have no solution in rational integers $b_1, \ldots, b_s$ of absolute values not exceeding $B \geq 2$.

This gives

$$\left| \frac{p_1^{j_1} \cdots p_s^{j_s}}{p_1^{h_1} \cdots p_s^{h_s}} - 1 \right| > \exp(-e^{2c_3 s_j} \Omega \log B) \tag{3.4}$$

where $\Omega \leq (\log P)^{2s_j}$, $B \leq \frac{\log(n+k)}{\log 2}$. It follows from (3.3) and (3.4) that

$$\frac{\log n}{\log_2 n} \ll \frac{\log(n/k)}{\log_2 n} \ll e^{2c_3 s_j} (\log P)^{2s_j}.$$

This implies

$$\log_2 n \ll s_j \log_2 P.$$

Without loss of generality we may assume $P \leq (\log_2 n)^3$. Hence, for n sufficiently large, by $n > \exp_2 k$,

$$s_j \gg \frac{\log_2 n}{\log_4 n} > 2\pi(k).$$

It follows that $n+j$ for $j=0,\dots,k-1, j\neq h$ contains $\gg \frac{\log_2 n}{\log_4 n}$ distinct prime factors $>k$. Since two such numbers $n+j$ cannot both be divisible by the same prime $>k$, we find

$$\omega(n,k) \gg k\frac{\log_2 n}{\log_4 n}.$$

Thus, by the Prime Number Theorem,

$$P(n,k) \gg k\log_2 n\frac{\log_3 n}{\log_4 n}.$$

4 The Number of Distinct Prime Factors

4.1 Complete Results

For more details we refer to [22]. Sylvester's earlier mentioned result implies that

$$\omega(n,k) > \pi(k)$$

if $n>k$. Let $\delta(k)=2$ for $3\le k\le 6, =1$ for $7\le k\le 16$, and $=0$ otherwise. Laishram and Shorey [23] improved upon earlier results by specifying all the finitely many exceptions to the inequality

$$\omega(n,k) \ge \pi(k) + \left[\frac{3}{4}\pi(k)\right] - 1 + \delta(k).$$

As corollaries they obtained

$$\textit{If } (n,k)\notin\{(114,109),(114,113)\}, \textit{ then } \omega(n,k)\ge \pi(k)+\left[\frac{2}{3}\pi(k)\right]-1$$

and

$$\omega(n,k)\ge \min\left(\pi(k)+\left[\frac{3}{4}\pi(k)\right]-1+\delta(k), \pi(2k)-1\right).$$

They further proved

$$\textit{If } (n,k)\neq(6,4) \textit{ and } 12n>17k, \textit{ then } \omega(n,k)\ge\pi(2k).$$

Again this is best possible, in view of $\omega(6,4)=\pi(8)-1$ and $\omega(34,24)=\pi(48)-1$.

4.2 Asymptotic Results

Ramachandra et al. [32] proved that there exists a constant $c_4 > 0$ such that for $n > \exp(c_4(\log k)^2)$,

$$\omega(n,k) > k.$$

Shorey and Tijdeman [37, Theorem 5] showed that there exists a constant $c_5 > 0$ such that for $k > c_5, n > \exp_2(c_5 k)$,

$$\omega(n,k) > k + \pi(k) - 2.$$

5 The Greatest Squarefree Divisor

There are hardly estimates on $R(n,k)$ in the literature, but the best approach seems to be the following. Combine the results of the previous section with estimates on the product of the first primes. For the complete results an explicit estimate is required, e.g.
the product of the primes $\le r$ *is less than* 3^r, see [18].
For the asymptotic results the best possible result reads
the product of the primes $\le r$ *is* $e^{(1+o(1))r}$,
which follows from the proof of the Prime Number Theorem. It follows that the product of the first t primes is $t^{(1+o(1))t}$. Thus, as an example, from the first result of Sect. 4.2, we have for $n > \exp(c_4(\log k)^2)$,

$$R(n,k) \ge k^{(1+o(1))k}.$$

6 The m-th Powerfree Part

Khodzhaev [21] answered a question of Sprindzhuk by showing that there exists a positive constant c_6 such that there are only finitely many pairs of integers (n,k) with $k < (\log n)^{c_6}$ for which

$$Q_2(n,k) < k^k. \tag{6.1}$$

More precisely, he showed that there exist positive constants c_7, c_8 such that (6.1) does not hold when $1 \le k \le c_7\sqrt{n}$, but (6.1) holds for all $k \ge c_8\sqrt{n}$.

Sprindžuk [41] and Turk [44] gave bounds for the greatest m-free part of a polynomial $f(x) \in \mathbb{Z}[x]$ at integers x. These bounds imply, for $k \ge 3$,

$$Q_2(n,k) \gg_{\varepsilon,k} (\log n)^{\frac{1}{12}-\varepsilon}.$$

(cf. [41, p. 161], formula (2.10)) and for $k \geq 3, m \geq 3$,

$$Q_m(n,k) > c_9^{-m^2} (\log n)^{1/(2m^2\phi(m))},$$

where $c_9 > 0$ depends only on k and $\phi(m)$ is the Euler function (cf. [41, p. 139], formula (1.2)).

It follows from a result of Turk [44] on polynomial values that for $k \geq 3, m \geq 2$, $n > 20$

$$P(Q_m(n,k)) \gg_k \log_2 n$$

and for $k = 2, m \geq 3$,

$$P(Q_m(n,k)) \gg \log_3 n.$$

de Weger and van de Woestijne [9] considered

$$\lambda_m(n,k) = \max_{i=0,1,\ldots,k-1} Q_m(n-i).$$

They proved that for $k \geq 2, m \geq 3$ and all $n \in \mathbb{N}$

$$\lambda_m(n,k) \gg_{k,m} (\log n)^{1/(2m-1)}. \tag{6.2}$$

On the other hand, they showed that there are infinitely many pairs k, m such that

$$\lambda_m(n,k) \ll_{k,m} n^{1-m/(km-1)}.$$

If k and m are odd, the exponent may be replaced by $1 - m/(km-2)$. In Sect. 8 we argue that it is likely that the last two results are close to the best possible ones.

In order to obtain a lower bound for $Q_m(n,k)$ from (6.2) we first remark that (6.2) implies

$$\prod_{i=0}^{k-1} Q_m(n,k) \gg_{k,m} (\log n)^{k/(2m-1)}$$

and then have to correct for the common factors. By an argument of Erdős [11] it suffices to divide by

$$\prod_{p<k} p^{[\frac{k}{p}]+[\frac{k}{p^2}]+\cdots} < k! \tag{6.3}$$

which depends only on k. It follows from (6.2) and (6.3) that

$$Q_m(n,k) \gg_{k,m} (\log n)^{k/(2m-1)}.$$

The exponent of $\log n$ is much better than in the earlier mentioned results of Sprindžuk.

7 The Erdős–Woods Conjecture

Erdős [12] conjectured that if m, n are positive integers there exists a k such that if for $1 \le i \le k$ the numbers $m+i$ and $n+i$ have the same prime factors, then $m = n$. This problem is equivalent with a problem of J. Robinson in logic (Woods [46]). The only known examples of positive integers (m, n, k) with $1 \le m < n, k \ge 2$ and

$$R(m+i) = R(n+i) \text{ for } 0 \le i < k \tag{7.1}$$

arise from

$$R(2^h - 2) = R(2^h(2^h - 2)), R(2^h - 1) = R((2^h - 1)^2) \ \ (h \ge 2)$$

and

$$R(75) = R(1215) = 15, R(76) = R(1216) = 38.$$

It is proved in [4] that if (7.1) holds then

$$\log k \ll (\log m \log_2 m)^{1/2} \ \text{ for } k \ge 3,$$

$$\log(n-m) \gg k(\log k)^2/\log_2 k \ \text{ for } k \ge 3,$$

and

$$\log(n-m) \gg k(\log k + \log_3 n)\log_2 y(\log_3 y)^{-1} \ \text{ for } k \ge 27.$$

8 Results Under the *abc*-Conjecture

The well-known *abc*-conjecture reads as follows.

Conjecture 1 For any given $\varepsilon > 0$ and coprime positive integers a, b, c satisfying $a + b = c$ we have

$$c \ll_\varepsilon R(abc)^{1+\varepsilon}.$$

In this section we give applications of this conjecture.

8.1 Estimates for Fixed k

Langevin [27] (see also Granville [16]) proved that if the *abc*-conjecture is true and $g(x) \in \mathbb{Z}[x]$ has no repeated roots, then for any $\varepsilon > 0$ we have $\prod_{p|g(n)} p \gg |n|^{\deg(g)-1-\varepsilon}$. It follows from this result that under the *abc*-conjecture

$$R(n,k) \gg_k |n|^{k-1-\varepsilon}. \tag{8.1}$$

de Weger and van de Woestijne [9] showed that for any $\varepsilon > 0, k \geq 2, m \geq 2$ under the *abc*-conjecture there are only finitely many integers n for which

$$\lambda_m(n,k) \leq n^{1-\frac{m}{km-k}-\varepsilon}. \tag{8.2}$$

This is a very good counterpart to their unconditional results with exponent $1 - m/(km-1)$ and $1 - m/(km-2)$ mentioned in Sect. 6. It follows from (8.2) that

$$\prod_{i=0}^{k-1} Q_m(n+i) \gg n^{k-\frac{m}{m-1}-k\varepsilon}.$$

In order to obtain a lower bound for $Q_m(n,k)$ we need to correct for the common factors. By the argument of Erdős (6.3) the common factor depends only on k. Thus, for any $\varepsilon > 0$,

$$Q_m(n,k) \gg_{k,m,\varepsilon} n^{k-1-\frac{1}{m-1}-\varepsilon}. \tag{8.3}$$

Note that, apart from ε, both (8.1) and (8.3) for $k = 2$ are the best possible. For (8.1) it suffices to observe that n can be a power of 2 and the other terms are at most $n + k$, for (8.3) that $x = n + 1, y = n$ can be a solution of the Pell equation $x^2 - 2y^2 = 1$.

We shall prove (8.1), (8.3) and a related result by a new method based on the following lemma which may have some independent interest.

Lemma 8.1 *Let k be a positive integer. Let x be a positive real variable. Then*

$$\prod_{\text{even } i=0}^{k} (x+i)^{\binom{k}{i}} - \prod_{\text{odd } i=0}^{k} (x+i)^{\binom{k}{i}} = -(k-1)!x^{2^{k-1}-k} + O_k(x^{2^{k-1}-k-1}).$$

Proof The following formula holds for Stirling numbers of the second kind:

$$S_{n,k} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n.$$

We have $S(n,n) = 1$ and $S(n,k) = 0$ for $k > n$ (see, e.g., [1, pp. 824–825]). It follows that, as $x \to 0$,

$$\sum_{i=0}^{k}(-1)^i\binom{k}{i}\log(1+ix) = \sum_{i=0}^{k}(-1)^i\binom{k}{i}\sum_{j=1}^{\infty}(-1)^{j-1}\frac{i^jx^j}{j} =$$

$$\sum_{j=1}^{\infty}\frac{(-1)^{k-j-1}x^j}{j}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^j = -(k-1)!x^k + O_k(x^{k+1}).$$

Hence

$$\frac{\prod_{i \text{ even},\ i=0}^{k}(1+ix)^{\binom{k}{i}}}{\prod_{i \text{ odd},\ i=0}^{k}(1+ix)^{\binom{k}{i}}} - 1 = -(k-1)!x^k + O_k(x^{k+1}).$$

Since $\sum_{i=0}^{k}(-1)^i\binom{k}{i} = (1-1)^k = 0$, we obtain, for $x \to \infty$,

$$\frac{\prod_{i \text{ even},\ i=0}^{k}(x+i)^{\binom{k}{i}}}{\prod_{i \text{ odd},\ i=0}^{k}(x+i)^{\binom{k}{i}}} - 1 = -(k-1)!x^{-k} + O_k(x^{-k-1}).$$

Thus, using that $\sum_{i \text{ odd},\ i=0}^{k}\binom{k}{i} = 2^{k-1}$,

$$\prod_{i \text{ even},\ i=0}^{k}(x+i)^{\binom{k}{i}} - \prod_{i \text{ odd},\ i=0}^{k}(x+i)^{\binom{k}{i}} = -(k-1)!x^{2^{k-1}-k} + O_k(x^{2^{k-1}-k-1}).$$

Theorem 8.2 *Let k, m and n be integers with $n \geq k \geq 2, m \geq 2$. Then, assuming the abc-conjecture, for every $\varepsilon > 0$ we have*

(a) $Q_m(n,k) \gg_{\varepsilon,k,m} n^{k-1-\frac{1}{m-1}-\varepsilon}$,
(b) $R(n,k) \gg_{\varepsilon,k} n^{k-1-\varepsilon}$,
(c) $P(n,k) \geq (k-1+o_k(1))\log n$.

Proof (a) We apply the *abc*-conjecture to

$$\frac{1}{g}\prod_{\text{even } i=0}^{k-1}(n+i)^{\binom{k-1}{i}} - \frac{1}{g}\prod_{\text{odd } i=0}^{k-1}(n+i)^{\binom{k-1}{i}} = O_k(n^{2^{k-2}-k+1}),$$

where g is the greatest common divisor of the first two terms. By the argument (6.3) of Erdős, $g = O_k(1)$. Hence, by $AB^m = N \ll_k n^k$,

$$n^{2^{k-2}} \ll_{\varepsilon,k} \left(R(AB)\cdot n^{2^{k-2}-k+1}\right)^{1+\varepsilon} \ll_{\varepsilon,k} \left(A^{\frac{m-1}{m}}n^{2^{k-2}-k+1+\frac{k}{m}}\right)^{1+\varepsilon}. \tag{8.4}$$

It follows that

$$A \gg_{\varepsilon,k,m} n^{k-1-\frac{1}{m-1}-\varepsilon\frac{m}{m-1}2^{k-2}}.$$

(b) It follows from (8.4) that

$$R(AB) \gg_{\varepsilon,k} n^{k-1-\varepsilon\cdot 2^{k-2}}.$$

(c) Since the product of the first l primes is $e^{(1+o(1))l}$, we deduce from part (b) that $P(n,k) \geq (k-1+o_k(1))\log n$.

8.2 Estimates for General n, k

8.2.1 Greatest Prime Factor

Theorem 8.3 *Let $0 < \varepsilon < 1/2$ and $n > k^{3/2}$. Then under the abc-conjecture, there exists a number k_1 depending only on ε such that for $k \geq k_1$ we have*

$$P(n,k) \geq (\frac{1}{2} - \varepsilon)k\log n.$$

Proof Let $k \geq k_1$. Assume that

$$P(n,k) < \left(\frac{1}{2} - \varepsilon\right) k\log n. \tag{8.5}$$

Then, for a suitable constant c_{10}, by the Prime Number Theorem with remainder term,

$$\omega(n,k) \leq \frac{(\frac{1}{2}-\varepsilon)k\log n}{\log k + \log_2 n} + \frac{c_{10}k\log n}{(\log k + \log_2 n)^2} \leq \frac{(\frac{1}{2}-\frac{\varepsilon}{2})k\log n}{\log k + \log_2 n}. \tag{8.6}$$

For $0 \leq i < k$, write

$$n + i = A_i B_i$$

with $P(A_i) \leq k$ and $\gcd(B_i, \prod_{p\leq k} p) = 1$. For every prime $p \leq k$, let i_p with $0 \leq i_p < k$ be such that p appears to the maximum power in A_{i_p}. Let S_1 be the set obtained from $\{0, 1, \ldots, k-1\}$ by deleting i_p for each prime $p \leq k$. Then $|S_i| \geq k - \pi(k)$. By the combinatorial argument (6.3) of Erdős,

$$\prod_{A_i \in S_1} A_i \leq k^k. \tag{8.7}$$

Suppose that there exist at most $(1-\frac{\varepsilon}{4})k$ number of i's in S_1 such that

$$A_i \le k^{8/\varepsilon}.$$

Then there are at least $\varepsilon k/8$ number of i's with $A_i > k^{8/\varepsilon}$. Consequently, from (8.7) we get

$$k^k \ge \prod_{i\in S_1} a_i > (k^{8/\varepsilon})^{\varepsilon k/8} = k^k,$$

a contradiction. Thus there exists a set $S_2 \subseteq S_1$ with $|S_2| > (1-\frac{\varepsilon}{4})k$ and

$$A_i \le k^{8/\varepsilon} \ \text{ for } \ i \in S_2.$$

Assume that there is at most one B_i with $i \in S_2$ such that

$$\omega(B_i) \le \frac{(\frac{1}{2}-\frac{\varepsilon}{3})\log n}{\log k + \log_2 n}.$$

Then

$$\omega(n,k) \ge \sum_{i\in S_2} \omega(B_i) \ge \frac{(\frac{1}{2}-\frac{\varepsilon}{3})k\log n}{\log k + \log_2 n}\left((1-\frac{\varepsilon}{4})k - 1\right).$$

From (8.6) we get

$$\frac{(\frac{1}{2}-\frac{11\varepsilon}{24})k\log n}{\log k + \log_2 n} \le \frac{(\frac{1}{2}-\frac{\varepsilon}{2})k\log n}{\log k + \log_2 n}.$$

Thus there exist at least two B_i's, say B_{i_1} and B_{i_2}, with $i_1, i_2 \in S_2, i_1 > i_2$ and

$$\omega(B_{i_j}) \le \frac{(\frac{1}{2}-\frac{\varepsilon}{3})\log n}{\log k + \log_2 n}, \ \ j = 1, 2.$$

By (8.5) we get

$$R(B_{i_j}) \le (k\log n)^{\frac{(\frac{1}{2}-\frac{\varepsilon}{3})\log n}{\log k + \log_2 n}} \le n^{\frac{1}{2}-\frac{\varepsilon}{3}}.$$

Applying the abc-conjecture to

$$n + i_1 = n + i_2 + (i_1 - i_2)$$

we get

$$n \le c_{11}(R((n+i_1)(n+i_2))k)^{1+\frac{\varepsilon}{2}} \le c_{11}(R(A_{i_1}B_{i_1}A_{i_2}B_{i_2})k)^{1+\frac{\varepsilon}{2}}$$
$$\le c_{11}(k^{\frac{17}{\varepsilon}}n^{(1-\frac{2\varepsilon}{3})})^{1+\frac{\varepsilon}{2}} \le c_{11}k^{\frac{17}{\varepsilon}(1+\frac{\varepsilon}{2})}n^{1-\frac{\varepsilon}{6}},$$

where c_{11} is a constant depending only on ε. Therefore,

$$\log n \le \frac{6}{\varepsilon}\log c_{11} + \frac{102}{\varepsilon^2}\left(1+\frac{\varepsilon}{2}\right)\log k \le c_{12}\log k \tag{8.8}$$

where c_{12} depends only on ε. By (3.1) and (8.8) we get

$$P(n,k) \gg k\log k\frac{\log_2 k}{\log_3 k} \gg k\log n\frac{\log_2 n}{\log_3 n}.$$

Hence the assertion follows.

9 Proof of the Erdős–Woods Conjecture Under the Explicit *abc*-Conjecture

As a special case of a result on the analogue of the Erdős–Woods conjecture for arithmetic progressions it was proved in [5] that under assumption of the *abc*-conjecture the original Erdős–Woods conjecture admits only finitely many exceptions for every $k > 2$. (See [5, Proposition 1].) For $k = 2$ there exist infinitely many solutions: for every integer $h \ge 2$ the pairs $(2^h - 2, 2^h(2^h - 2))$ and $(2^h - 1, (2^h - 1)^2)$ have the same prime divisors.

An explicit version of the *abc*-conjecture is the following.

Conjecture 2 (Baker, [2]) Let a, b, and c be pairwise coprime integers satisfying $a + b = c$. Then

$$c < \frac{6}{5}R(abc)\frac{(\log R(abc))^{\omega(abc)}}{\omega(abc)!}. \tag{9.1}$$

Laishram and Shorey [25] proved that a consequence of (9.1) is that

$$c < (R(abc))^{7/4}. \tag{9.2}$$

Here we prove the complete Erdős–Woods conjecture for $k \ge 3$ under assumption of the explicit *abc*-conjecture. Of course, it suffices to prove it for $k = 3$.

Theorem 9.1 *Assume Conjecture 2. Then there are no positive integers $n_1 < n_2$ such that for $i = 0, 1, 2$ the numbers $n_1 + i$ and $n_2 + i$ have the same prime divisors.*

Proof Apply Conjecture 2 with (9.2) in place of (9.1) to the equation $(n_2 + 1)^2 - n_2(n_2 + 2) = 1$. This yields

$$n_2^2 < (R(n_2(n_2 + 1)(n_2 + 2)))^{1.75}.$$

Observe that every prime p dividing $n_2(n_2 + 1)(n_2 + 2)$ divides either $n_2 - n_1$ or $(n_2 + 1) - (n_1 + 1)$ or $(n_2 + 2) - (n_1 + 2)$. Thus

$$R(n_2(n_2 + 1)(n_2 + 2)) \le n_2 - n_1 < n_2.$$

Combining the inequalities we obtain

$$n_2^2 < n_2^{1.75},$$

a contradiction.

10 Generalizations

More general results have been obtained for the greatest prime factor of the product of the terms of a finite arithmetical progression (see e.g. [24, 36]) and for the greatest prime factor of the value of a polynomial or binary form (see, e.g., [40]), for the number of distinct prime divisors of the product of the terms of a finite arithmetical progression (see, e.g., [22]) and of a polynomial value (see, e.g., [43]), for the greatest m-free part of a polynomial value (see [44]) and for the analogue of the Erdős–Woods conjecture for an arithmetical progression (see [5]).

There are also more general results under the assumption that the *abc*-conjecture is true: for lower bounds for the greatest squarefree divisor of a polynomial value and a binary form value, see [10, 16, 27], for a lower bound for the greatest m-free part of a binary form value, see [27], and for the Erdős–Woods conjecture for an arithmetical progression, see [5].

Finally, for an estimate for the number of prime divisors of a product of consecutive integers under the assumption that Schinzel's Hypothesis H is true, see [6].

References

1. M. Abramowitz, I.A. Stogun, *Handbook of Mathematical Functions* (Dover Publications, New York, 1972)
2. A. Baker, Experiments on the *abc*-conjecture. Publ. Math. Debr. **65**, 253–260 (2004)

3. R.C. Baker, G. Harman, J. Pintz, The difference between consecutive primes II. Proc. Lond. Math. Soc. (3) **83**, 532–562 (2001)
4. R. Balasubramanian, T.N. Shorey, M. Waldschmidt, On the maximal length of two sequences of consecutive integers with the same prime divisors. Acta Math. Hung. **54**, 225–236 (1989)
5. R. Balasubramanian, M. Langevin, T.N. Shorey, M. Waldschmidt, On the maximal length of two sequences of integers in arithmetic progressions with the same prime divisors. Monatsh. Math. **121**, 295–307 (1996)
6. R. Balasubramanian, S. Laishram, T.N. Shorey, R. Thangadurai, The number of prime divisors of a product of consecutive integers. J. Combin. Number Theory **1**, 253–261 (2009)
7. M. Bauer, M.A. Bennett, On a question of Erdős and Graham. Enseign. Math. (2) **53**, 259–264 (2007)
8. M.A. Bennett, R. van Luijk, Squares from blocks of consecutive integers: a problem of Erdős and Graham. Indag. Math. (N.S.) **23**, 123–127 (2012)
9. B.M.M. de Weger, C.E. van de Woestijne, On the power-free parts of consecutive integers. Acta Arith. **90**, 387–395 (1999)
10. N. Elkies, *ABC* implies Mordell. Int. Math. Res. Not. **7**, 99–109 (1991)
11. P. Erdős, On the product of consecutive integers, (III). Indag. Math. **17**, 85–90 (1955)
12. P. Erdős, How many pairs of products of consecutive integers have the same prime factors. Am. Math. Mon. **87**, 391–392 (1980)
13. P. Erdős, R.L. Graham, *Old en New Problems and Results in Combinatorial Number Theory*. L'Enseignement Mathématique, vol. 28 (L'Enseignement Mathématique, Geneva, 1980)
14. M. Filaseta, O. Trifonov, The irreducibility of the Bessel polynomials. J. Reine Angew. Math. **550**, 125–140 (2002)
15. C. Fuchs, T.N. Shorey, Divisibility properties of generalized Laguerre polynomials. Indag. Math. N.S. **20**, 217–231 (2009)
16. A. Granville, *ABC* allows us to count squarefrees. Int. Math. Res. Not. **1998**, 991–1009 (1998)
17. G. Hanrot, N. Saradha, T.N. Shorey, Almost perfect powers in consecutive integers. Acta Arith. **99**, 13–25 (2001)
18. D. Hanson, On the product of the primes. Can. Math. Bull. **15**, 33–37 (1972)
19. G. Harman, *Prime-detecting Sequences*. London Mathematical Society Monographs Series, vol. 33 (Princeton University Press, Princeton, 2007)
20. C. Jia, M.-C. Liu, On the largest prime factor of integers. Acta Arith. **95**, 17–48 (2000)
21. N.M. Khodzhaev, The problem of V.G. Sprindžuk on the square-free part of the product of consecutive natural numbers (Russian). Vestnik Moskov. Univ. Ser. I Mat. Mekh. **78**(1), 3–7 (1997); translation in Moscow Univ. Math. Bull. **52**(1), 1–5 (1997)
22. S. Laishram, Some topics in number theory (Refinements, extensions and generalisations of a theorem of Sylvester on the prime factors of a product of consecutive integers), Ph.D. thesis, TIFR Mumbai, 2007
23. S. Laishram, T.N. Shorey, The greatest prime factor of a product of consecutive integers. Acta Arith. **120**, 299–306 (2005)
24. S. Laishram, T.N. Shorey, The greatest prime divisor of a product of terms in an arithmetic progression. Indag. Math. (N.S.) **17**, 425–436 (2006)
25. S. Laishram, T.N. Shorey, Baker's explicit *abc*-conjecture and applications. Acta Arith. **155**, 419–429 (2012)
26. M. Langevin, Plus grand facteur premier d'entiers voisins. C.R. Acad. Sci. Paris **281**, A491–A493 (1975)
27. M. Langevin, *Partie sans facteur carré de* $F(a, b)$ *(modulo la conjecture (abc)).* Séminaire Théorie des Nombres (1993–1994), Publ. Math. Univ. Caen.
28. F. Luca, P.G. Walsh, On a Diophantine equation related to a conjecture of Erdős and Graham. Glas. Mat. Ser. III **42**(62), 281–289 (2011)

29. E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II (Russian). Izv. Ross. Akad. Nauk Ser. Mat. **64**(6), 125–180 (2000); English transl.: Izv. Math. **64**, 1217–1269 (2000)
30. S.G. Nair, T.N. Shorey, Sharpening of a lower bound for the greatest prime factor of consecutive integers with application to equation $n! = a_1!a_2! \cdot a_t!$ (to appear)
31. K. Ramachandra, Application of Baker's theory to two problems considered by Erdős and Selfridge. J. Indian Math. Soc. (N.S.) **37**, 25–34 (1973/1974)
32. K. Ramachandra, T.N. Shorey, R. Tijdeman, On Grimm's problem relating to factorisation of a block of consecutive integers II. J. Reine Angew. Math. **288**, 192–201 (1976)
33. J.W. Sander, On numbers with a large prime power factor. Acta Math. Hung. **63**, 149–165 (1994)
34. T.N. Shorey, On gaps between numbers with a large prime factor II. Acta Arith. **25**, 365–373 (1974)
35. T.N. Shorey, Yu.V. Nesterenko, Perfect powers in products of integers from a block of consecutive integers II. Acta Arith. **76**, 191–198 (1996)
36. T.N. Shorey, R. Tijdeman, On the greatest prime factor of an arithmetical progression II. Acta Arith. **53**, 499–504 (1990)
37. T.N. Shorey, R. Tijdeman, On the number of prime factors of a finite arithmetical progression. Acta Arith. **61**, 375–390 (1992)
38. T.N. Shorey, R. Tijdeman, Prime factors of arithmetic progressions and binomial coefficients, *Diophantine Geometry*. CRM Series, vol. 4 (Edizioni della Normale, Pisa, 2007), pp. 283–296
39. T.N. Shorey, R. Tijdeman, Generalizations of some irreducibility results by Schur. Acta Arith. **145**, 341–371 (2010)
40. T.N. Shorey, A.J. van der Poorten, R. Tijdeman, A. Schinzel, Applications of the Gel'fond-Baker method to Diophantine equations, in *Transcendence Theory: Advances and Applications*, ed. by A. Baker, D.W. Masser (Academic, London, 1977), pp. 59–77
41. V.G. Sprindžuk, *Classical Diophantine Equations*. Lecture Notes in Mathematics, vol. 1559 (Springer, Berlin, 1993). (Original version in Russian: *Klassicheskie diofantovy uravneniya ot dvukh neizvestnykh*, Nauka, Moscow, 1982)
42. R. Tijdeman, Exponential Diophantine equations 1986–1996, in *Number Theory (Eger, 1996)* (de Gruyter, Berlin, 1998), pp. 523–539
43. J. Turk, Prime divisors of polynomials at consecutive integers. J. Reine Angew. Math. **319**, 142–152 (1980)
44. J. Turk, Polynomial values and almost powers. Mich. Math. J. **29**, 213–220 (1982)
45. M. Ulas, On products of disjoint blocks of consecutive integers. Enseign. Math. **51**, 331–334 (2005)
46. A.R. Woods, Some problems in logic and number theory and its connections, Ph.D. thesis, University of Manchester, Manchester, 1981

The GCD of the Shifted Fibonacci Sequence

Jürgen Spilker

Dedicated to my friend Wolfgang Schwarz

Abstract Let $f(n)$ be the Fibonacci-sequence defined by $f(n+2) = f(n)+f(n+1)$, $f(0) = 0, f(1) = 1$, and let $t_s(n) := \gcd(f(n)+s, f(n+1)+s)$, s integer. In 2011 K.-W. Chen has proved that the function $t_s(n)$ is bounded if s exceeds 1. THEOREM: *Let n and s be integers.* (1) *$t_s(n)$ divides $s^2 + (-1)^n$;* (2) *if $m := s^4 - 1$ is not 0, then $t_s(n)$ is simply periodic; a period p is defined by $f(p) \equiv 0 \bmod m$, $f(p+1) \equiv 0 \bmod m$.* There are explicit formulas of $t_s(n)$ and generalisations to a wider class of recursive second-order sequences.

Keywords Fibonacci sequence • Recurrences

2010 Mathematics subject classification: Primary 11B39; Secondary 11B37

1 Introduction

The Fibonacci sequence $f : \mathbb{N}_0 \to \mathbb{N}_0$ is defined by the recursion

$$f(n+2) = f(n) + f(n+1), \quad n \in \mathbb{N}_0 \tag{1.1}$$

and the initial conditions $f(0) = 0, f(1) = 1$. Any two successive terms of the sequence are coprime, since by (1.1) every common divisor $d > 0$ of $f(n+1)$ and $f(n+2)$ divides $f(n)$, then $f(n-1), \ldots, f(1)$, so $d = 1$.

In this note we consider the shifted sequence and define the greatest common divisor (gcd)

$$t_s(n) := (f(n) + s, f(n+1) + s), \quad n \in \mathbb{N}_0, s \in \mathbb{Z}.$$

J. Spilker (✉)
Mathematisches Institut, Albert-Ludwigs-Universität, Eckerstr. 1, 79104 Freiburg i. Br., Germany
e-mail: juergen.spilker@t-online.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_28

The function $n \mapsto t_0(n)$ is constant. The function $n \mapsto t_1(n)$ is unbounded, since

$$(f(4n-1)+1, f(4n)+1) = f(2n-1) \geq n, \quad n \in \mathbb{N}$$

(in Lemma 4.1 replace n by $4n-1$ and specialize $g(n) = f(n), m = -2, k = n$). All other gcd-functions $t_s(n)$ with $|s| > 1$ "behave between these extremes": they are bounded [1].

In this article we will show that they are in fact simply periodic. This result will be generalized to a class of functions f and general shifts

$$n \mapsto (f(n)+s, f(n+r)+t), \quad r, s, t \in \mathbb{Z}, r > 0.$$

(Theorems 2.1 and 2.6). It is astonishing that these multiplicatively defined functions have such an additive property.

If $f(n)$ is the Fibonacci sequence, in Theorem 2.2 we give formulas for $t_s(n)$, and compare right- and left-shifts in Theorem 2.4. The theorems are in Sect. 2, the proofs in Sects. 3–8; they are elementary.

The gcd of three shifted Fibonacci numbers is trivial:

$$(f(n)+s, f(n+1)+s, f(n+2)+s) = 1, \quad n, s \in \mathbb{Z}$$

since every divisor $d \in \mathbb{N}$ of these three integers divides

$$f(n+1)+s-(f(n)+s) = f(n-1)$$

and

$$f(n+2)+s-(f(n+1)+s) = f(n),$$

hence it divides $(f(n-1), f(n)) = 1$ and $d = 1$.

2 The Theorems

The periodicity of the gcd-function $t_s(n)$ is not only valid for the Fibonacci sequence, but also for a wider class of recursively defined functions.

Theorem 2.1 *Let $b, \alpha, \beta, s \in \mathbb{Z}, \gamma := \beta^2 - \alpha^2 - \alpha\beta b$ and $f : \mathbb{N}_0 \to \mathbb{Z}$ defined by*

$$f(n+2) = f(n) + bf(n+1), \quad f(0) = \alpha, f(1) = \beta. \tag{2.1}$$

Suppose that no integer $n \in \mathbb{N}_0$ satisfies $f(n) = f(n+1) = -s$. Then

$$t_s(n) := (f(n)+s, f(n+1)+s), \quad n \in \mathbb{N}_0,$$

is defined and we have

(a) $t_s(n)$ *divides* $bs^2 + (-1)^n\gamma, n \in \mathbb{N}_0$*;*
(b) if $m := |b^2s^4 - \gamma^2| \neq 0$*, then the function* $n \mapsto t_s(n)$ *is simply periodic, i.e., there exists* $p \in \mathbb{N}$ *so that* $t_s(n+p) = t_s(n), n \in \mathbb{N}_0$.

A period $p \leq m^2$ *can be chosen by*

$$f(p) \equiv 0 \; mod \; m, f(p+1) \equiv 1 \; mod \; m.$$

One can obtain formulas for $t_s(n)$.

Theorem 2.2 *Let* $f(n)$ *be the Fibonacci sequence,* $s \in \mathbb{Z}$ *and* $|s| > 1, k \in \mathbb{N}$.

(a) If $f(2k-i) \equiv \alpha_i \; mod \; (s^2+1), 0 \leq \alpha_i < s^2+1, i \in \{0,1\}$*, then*

$$t_s(4k) = (\alpha_0 + s\alpha_1, s\alpha_0 - \alpha_1, s^2+1),$$
$$t_s(4k-2) = (\alpha_0 + (s-1)\alpha_1, s\alpha_0 - (s+1)\alpha_1, s^2+1).$$

(b) If $f(2k-i) \equiv \beta_i \; mod \; (s^2-1), 0 \leq \beta_i < s^2-1, i \in \{0,1\}$*, then*

$$t_s(4k-1) = ((s+1)\beta_1, (s-1)\beta_0 - s\beta_1, s^2-1),$$
$$t_s(4k-3) = (\beta_0 - (s+2)\beta_1, (s-1)\beta_0 - (s-1)\beta_1, s^2-1).$$

Periodical functions have a mean-value M. The next theorem contains two formulas for M.

Theorem 2.3 *Let* $p \in \mathbb{N}$ *and* $t : \mathbb{N}_0 \to \mathbb{Z}$ *satisfies* $t(n+p) = t(n), n \in \mathbb{N}_0$. *Moreover, let* $q > 0$ *be the least common multiple of* $t(0), t(1), \ldots, t(p-1)$. *Then* $M(t) := \frac{1}{p}\sum_{0 \leq n \leq p-1} t(n)$ *satisfies*

$$M(t) = \frac{1}{p}\sum_{d|q} dl_1(d), \quad \text{where } l_1(d) := \#\{0 \leq n \leq p-1 : t(n) = d\}$$

and

$$M(t) = \frac{1}{p}\sum_{d|q} \varphi(d) l_2(d), \quad \text{where } l_2(d) := \#\{0 \leq n \leq p-1 : d \mid t(n)\};$$

here $\varphi(n)$ *is the Euler function.*

Example Let $f(n)$ be the Fibonacci sequence and $s \in \{-2, 2\}$. Theorem 2.1 gives $t_s(n) \in \{1, 3, 5\}, n \in \mathbb{N}_0$. In a table of the first Fibonacci numbers one finds

$$f(40) \equiv 0 \bmod 15, \quad f(41) \equiv 1 \bmod 15.$$

So $t_s(n+40) = t_s(n)$, if $n \geq 0$, and with the help of Theorem 2.2,

$$t_2(n) = \begin{cases} 5 & \text{if } n \equiv 6 \bmod 20 \\ 3 & \text{if } n \equiv 1 \bmod 8 \\ 1 & \text{else,} \end{cases} \qquad t_{-2}(n) = \begin{cases} 5 & \text{if } n \equiv 16 \bmod 20 \\ 3 & \text{if } n \equiv 5 \bmod 8 \\ 1 & \text{else.} \end{cases}$$

In Theorem 2.3, take $p = 40, q = 15$. Then for $t = t_2$ and $t = t_{-2}$,

$$l_1(d) = \begin{cases} 0 & , d = 15 \\ 2 & , d = 5 \\ 5 & , d = 3 \\ 33 & , d = 1, \end{cases} \qquad l_2(d) = \begin{cases} 0 & , d = 15 \\ 2 & , d = 5 \\ 5 & , d = 3 \\ 40 & , d = 1, \end{cases}$$

and $M(t_2) = M(t_{-2}) = \frac{29}{20}$.

In this example the gcd-functions $t_2(n)$ and $t_{-2}(n)$ have the same values on a period interval inclusive their multiplicity and they attain the upper bound s^2+1 on the even numbers, resp. $s^2 - 1$ on the odd integers. This has the following generalization.

Theorem 2.4 *Let $f(n)$ be the Fibonacci sequence, $s \in \mathbb{Z}, |s| > 1$ and $p \in 2\mathbb{N}$ a period of $t_s(n)$. Then the sequences $t_s(2), t_s(4), \ldots, t_s(p)$ and $t_{-s}(2), t_{-s}(4), \ldots, t_{-s}(p)$ are permutations of each other.*

Remark The restriction to even integers is necessary, since $t_3(7) = 8$, but $t_{-3}(n) \neq 8$ for every n.

Open Question *We have $M(t_2) = M(t_{-2}) = \frac{29}{20}, M(t_3) = \frac{34}{15}, M(t_{-3}) = \frac{8}{5}$. For which $s > 3$ is $M(t_s) = M(t_{-s})$?*

For every $m \in \mathbb{N}$ there exists an $i \in \mathbb{N}$ such that $m \mid f(i)$ [2, Theorem 1]. Then $e(m) := \min\{i \in \mathbb{N} : m \mid f(i)\}$ is called the entry point of m.

Theorem 2.5 *Let $f(n)$ be the Fibonacci sequence and $s \in \mathbb{Z}, |s| \geq 2$.*

(a) The function $n \mapsto t_s(n)$ has the upper bound $m = s^2 + 1$ as a value, iff the entry point $e = e(m)$ is odd and $s \equiv \pm f(e+1) \bmod m$.

(b) $t_s(n)$ has value $m = s^2 - 1$ on the odd integers iff $s = 2$, or e even and $s \equiv -f(e+1) \bmod m$.

Open Question *Let $f(n)$ be a solution of the general recursion*

$$f(n+2) = af(n) + bf(n+1), \quad a, b \in \mathbb{Z}.$$

If $|a| > 1$, is $t_s(n)$ still periodic?

The periodicity is also valid for a more general gcd-function.

Theorem 2.6 *Let $f(n)$ be the Fibonacci sequence and $r \in \mathbb{N}, s, t \in \mathbb{Z}, c := (-1)^{r+1}s^2 + (f(r+1) - f(r-1))st - t^2$. Assume that $f(n) = -s, f(n+r) = -t$ holds for no $n \in \mathbb{N}_0$, so that the function*

$$T(n) := (f(n) + s, f(n+r) + t), \quad n \in \mathbb{N}_0$$

is defined. Then

(a) $T(n)$ is a divisor of $c + (-1)^n f^2(r)$ for all $n \in \mathbb{N}_0$.
(b) If $|c| \neq f^2(r)$, the function $n \mapsto T(n)$ is simply periodic. A period $1 \leq p \leq m^2$ is found by

$$f(p) \equiv 0 \bmod m, \quad f(p+1) \equiv 1 \bmod m,$$

where $m := |c^2 - f^4(r)|$.

In the special case $t = -s$, there are formulas for

$$t_{s,-s} := (f(n) + s, f(n+1) - s).$$

Theorem 2.7 *Let $f(n)$ be the Fibonacci sequence, $s \in \mathbb{Z}, |s| > 1, k \in \mathbb{N}$.*

(a) Let $f(2k+i) \equiv \alpha_i \bmod (s^2+1), 0 \leq \alpha_i < s^2 + 1, i \in \{1, 2\}$. Then

$$t_{s,-s}(4k+1) = (\alpha_1 + s\alpha_2, s\alpha_1 - \alpha_2, s^2 + 1),$$
$$t_{s,-s}(4k+3) = (\alpha_1 + (s+1)\alpha_2, s\alpha_1 + (s-1)\alpha_2, s^2 + 1).$$

(b) Let $f(2k+i) \equiv \beta_i \bmod (s^2-1), 0 \leq \beta_i < s^2 - 1, i \in \{1, 2\}$. Then

$$t_{s,-s}(4k) = ((s+1)\beta_2 - \beta_1, (s-1)\beta_1, s^2 - 1),$$
$$t_{s,-s}(4k+2) = ((s+1)\beta_2, (s-1)\beta_1 - \beta_2, s^2 - 1).$$

The proof is similar to that of Theorem 2.2.

3 Proof of Theorem 2.1

We use the matrices

$$M := \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad F(n) := \begin{pmatrix} f(n+1) & f(n) \\ f(n) & f(n-1) \end{pmatrix}.$$

For every $n \in \mathbb{N}$,

$$F(n) = MF(n-1) = \ldots = M^{n-1}F(1).$$

Going over to determinants

$$f(n+1)f(n-1) - f^2(n) = (-1)^{n-1}(f(2)f(0) - f^2(1)) = (-1)^n\gamma.$$

Let $d \in \mathbb{N}$ be a common divisor of $f(n) + s$ and $f(n+1) + s$. Then

$$\begin{aligned} f(n+1)f(n-1) - f^2(n) &= f(n+1)(f(n+1) - bf(n)) - f^2(n) \\ &\equiv -bs^2 \bmod d. \end{aligned}$$

Consequently d is a divisor of $bs^2 + (-1)^n\gamma$. This proves assertion a.

The vector-valued mapping

$$n \mapsto \begin{pmatrix} f(n) \bmod m \\ f(n+1) \bmod m \end{pmatrix}$$

has only finite-many values. So there are integers p_1, p_2 such that $0 \le p_1 < p_2 \le m^2$ and

$$f(p_1) \equiv f(p_2) \bmod m, \quad f(p_1+1) \equiv f(p_2+1) \bmod m.$$

By (2.1) we get $f(p_1 + n) \equiv f(p_2 + n) \bmod m$ for every $n \ge 0$ and together with $p := p_2 - p_1 \le m^2$ we have

$$f(n+p) \equiv f(n) \bmod m \quad \text{for all } n \in \mathbb{N}_0.$$

Since by assertion a $t_s(n)$ divides m, for every $n \in \mathbb{N}_0$, we finally get

$$\begin{aligned} t_s(n) &= (f(n) + s, f(n+1) + s, m) \\ &= (f(n+p) + s, f(n+1+p) + s, m) = t_s(n+p). \end{aligned}$$

4 Proof of Theorem 2.2

The solutions $f : \mathbb{N}_0 \to \mathbb{Z}$ of (1.1) can be continued in exactly one way to functions $f : \mathbb{Z} \to \mathbb{Z}$ still with property (1.1). If $f(n)$ is the Fibonacci sequence, then

$$f(-n) = (-1)^{n+1}f(n), \quad n \in \mathbb{N}_0. \tag{4.1}$$

Lemma 4.1 *If $f, g : \mathbb{Z} \to \mathbb{Z}$ are solutions of (1.1) and $m, n, k \in \mathbb{Z}$, then*

$$(f(n)+g(m+1), f(n+1)-g(m)) = (f(n-2k)+g(m+2k+1), f(n-2k+1)-g(m+2k)).$$

Proof We use the following rules of the gcd

$$(a,b) = (b,a) = (-a,b), \quad (a,b) = (a+bc,b).$$

Let

$$t(n,m) := (f(n)+g(m+1), f(n+1)-g(m)).$$

Then by (1.1)

$$\begin{aligned} t(n,m) &= (f(n)+g(m+1), f(n-1)-g(m+2)) \\ &= (f(n-2)+g(m+3), f(n-1)-g(m+2)) = t(n-2,m+2). \end{aligned}$$

Iterating this we get the assertion $t(n,m) = t(n-2k, m+2k)$.

In Lemma 4.1 set $g(n) = sf(n), m = -2$. Then

$$t_s(n) = (f(n-2k)+sf(2k-1), f(n-2k+1)-sf(2k-2)).$$

First we consider the case $n \equiv 0 \bmod 4$, say $n = 4k$. Then

$$\begin{aligned} t_s(4k) &= (f(2k)+sf(2k-1), f(2k+1)-sf(2k-2)) \\ &= (f(2k)+sf(2k-1), -(s-1)f(2k)+(s+1)f(2k-1)) \\ &= (f(2k)+sf(2k-1), f(2k-1)-sf(2k)). \end{aligned}$$

Set $a_i := f(2k-i), i \in \{0,1\}$. Then $t_s(4k)$ is a divisor of a_0+sa_1 and a_1-sa_0, hence of $(a_0+sa_1)-s(a_1-sa_0) = (s^2+1)a_0$ and of $s(a_0+sa_1)+(a_1-sa_0) = (s^2+1)a_1$. Since a_0 and a_1 are coprime, $t_s(4k)$ divides s^2+1 (this is also a consequence of Theorem 2.1) and

$$\begin{aligned} t_s(4k) &= (a_0+sa_1, a_1-sa_0, s^2+1) \\ &= (\alpha_0+s\alpha_1, \alpha_1-s\alpha_0, s^2+1). \end{aligned}$$

This proves the assertion in the case $n = 4k$. The other cases $n \not\equiv 0 \bmod 4$ are proved in the same way.

5 Proof of Theorem 2.3

We have

$$pM(t) = \sum_{0\le n<p} t(n) = \sum_{d|q}\left(d \sum_{\substack{0\le n<p\\ t(n)=d}} 1\right) = \sum_{d|q} dl_1(d)$$

and further

$$pM(t) = \sum_{0\le n<p} (t(n),q) = \sum_{r|q}\left(r \sum_{\substack{0\le n<p\\ (t(n),q)=r}} 1\right) = \sum_{r|q}\left(r \sum_{\substack{0\le n<p\\ r|t(n)}} \sum_{l\left|\left(\frac{t(n)}{r},\frac{q}{r}\right)\right.} \mu(l)\right)$$

$$= \sum_{r|q} r\left(\sum_{l\left|\frac{q}{r}\right.} \mu(l) \sum_{\substack{0\le n<p\\ lr|t(n)}} 1\right) = \sum_{d|q}\left(\sum_{l|d} \mu(l)\frac{d}{l} \cdot \sum_{\substack{0\le n<p\\ d|t(n)}} 1\right).$$

Since $\varphi(d) = \sum_{l|d} \mu(l)\frac{d}{l}$, this is the second formula.

6 Proof of Theorem 2.4

If $n \in \mathbb{N}$ is an even integer, then with (4.1),

$$\begin{aligned} t_s(n) &= (f(n)+s, f(n+1)+s-f(n)-s) = (f(n)+s, f(n-1)) \\ &= (f(n-2)+s, f(n-1)) \\ &= (f(n-2)+s, f(n-1)-f(n-2)-s) = (f(n-2)+s, f(n-3)-s) \\ &= (-f(-n+2)+s, f(-n+3)-s) \\ &= (f(-n+2)-s, f(-n+3)-s) = t_{-s}(-n+2) \\ &= t_{-s}(-n+2+p). \end{aligned}$$

The mapping $\pi : n \mapsto -n+2+p$ is a bijection of the set $\{2,4,6,\dots,p\}$ and $t_s = t_{-s} \circ \pi$. This proves the theorem.

7 Proof of Theorem 2.5

With the help of the rule $f(m+n) = f(m+1)f(n) + f(m)f(n-1)$ we find that the integers $f(1), f(2), \ldots$ are modulo m equivalent to

$$\begin{aligned} &f(1), && f(2), \ldots, && f(e-1), 0, \\ &f(e+1)f(1), && f(e+1)f(2), \ldots, && f(e+1)f(e-1), 0, \\ &f^2(e+1)f(1), && f^2(e+1)f(2), \ldots, && f^2(e+1)f(e-1), 0, \ldots \end{aligned}$$

It follows that

$$f(ke) \equiv 0 \bmod m, \quad f(ke+1) \equiv f^k(e+1) \bmod m \quad (k \in \mathbb{N}). \tag{7.1}$$

Next the congruences

$$\begin{aligned} f(e+1) &= f(e) + f(e-1) \equiv f(e-1) \bmod m \\ f(e+1)f(e-1) &= f^2(e) + (-1)^e \equiv (-1)^e \bmod m \end{aligned}$$

give

$$f^2(e+1) \equiv (-1)^e \bmod m. \tag{7.2}$$

(a) Let $t_s(n_0) = m$. Since $t_s(n) = (f(n) + s, f(n-1))$, we have

$$f(n_0) + s \equiv 0 \bmod m, \quad f(n_0 - 1) \equiv 0 \bmod m. \tag{7.3}$$

By [2, Theorem 2.3], $n_0 - 1$ is a multiple of e, say $n_0 = ke + 1$ ($k \geq 0$). Now n_0 is an even integer, since otherwise $t_s(n_0) = s^2 + 1$ would divide $s^2 - 1$ (Theorem 2.1). Since k and e are odd, we get by (7.1) and (7.2)

$$f(n_0) = f(ke+1) \equiv f^k(e+1) \equiv (-1)^{\frac{k-1}{2}} f(e+1) \bmod m$$

and $s \equiv f(e+1) \bmod m$ or $s \equiv -f(e+1) \bmod m$. Conversely, if $s \equiv f(e+1) \bmod m$ and e is odd, then $n_0 := 3e+1$ is by (7.1) and (7.2), a solution of (7.3), hence m divides $t_s(n_0)$. By Theorem 2.1, $t_s(n_0)$ divides m, so $t_s(n_0) = m$. If $s \equiv -f(e+1) \bmod m$, then $n_0 := e + 1$ solves (7.3) and $t_s(n_0) = m$. This proves part a.

(b) In an analogous manner one shows part b.

8 Proof of Theorem 2.6

Let

$$F(n) := \begin{pmatrix} f(n+1) & f(n) \\ f(n) & f(n-1) \end{pmatrix} \quad \text{und} \quad M := F(1) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then

$$F(n) = MF(n-1) = M^2F(n-2) = \ldots = M^{n-1}F(1) = M^n.$$

Taking determinants gives

$$f(n+1)f(n-1) - f^2(n) = (-1)^n, \quad n \in \mathbb{N}_0. \tag{8.1}$$

Further

$$F(r+n) = M^{r+n} = M^r M^n = F(r)F(n).$$

Comparing the 1-2-elements in the matrices gives

$$f(n+r) = f(r+1)f(n) + f(r)f(n-1). \tag{8.2}$$

Let $d \in \mathbb{N}$ be a common divisor of $f(n) + s$ and $f(n+r) + t$. Then we have mod d

$$s \equiv -f(n), \quad t \equiv -f(n+r), \quad st \equiv f(n)f(n+r).$$

Together with (8.1) and (8.2) we compute mod d

$$\begin{aligned}
&(f(r+1) + f(r-1))st - t^2 \\
&\equiv [(f(r+1) + f(r-1))f(n) - f(n+r)]f(n+r) \\
&= (f(r-1)f(n) - f(r)f(n-1))(f(r+1)f(n) + f(r)f(n-1)) \\
&= f(r-1)f(r+1)f^2(n) - f(r)f(n-1)(f(r)f(n-1) + \\
&\quad + (f(r+1) - f(r-1))f(n)) \\
&= f(r-1)f(r+1)f^2(n) - f^2(r)f(n-1)f(n+1) \\
&= (f^2(r) + (-1)^r)f^2(n) - f^2(r)(f^2(n) + (-1)^n) \\
&\equiv (-1)^r s^2 - (-1)^n f^2(r), \qquad\qquad n \in \mathbb{N}_0
\end{aligned}$$

and finally

$$c + (-1)^n f^2(r) \equiv 0 \bmod d.$$

The second part of the theorem is proved like Theorem 2.2b.

References

1. K.-W. Chen, Greatest common divisors in shifted Fibonacci sequences. J. Integer. Seq. **14**, Art.11.4.7 (2011)
2. D.D. Wall, Fibonacci sequences modulo *m*. Am. Math. Mon. **67**, 525–532 (1960)

On Liouville Numbers: Yet Another Application of Functional Analysis to Number Theory

Jörn Steuding

Wie dem Geiste nichts zu groß ist, so ist der Güte nichts zu klein.
–Jean Paul

Abstract In 1962, Erdős proved that every real number can be represented as a sum and as a product of two Liouville numbers. This has been generalized by Rieger and Schwarz. In this note we shall give an analysis of these results and their proofs. Moreover, we consider a certain subclass of Liouville numbers and prove similar results for this subclass. Since Wolfgang Schwarz had been very much interested in the history of mathematics, and the author shares this interest, he could not resist to include a few historical remarks (and footnotes) on transcendental numbers and Baire's category theorem which might be interesting for the reader.

Keywords Baire's theorem • Liouville numbers

2010 Mathematics subject classification: Primary 11J81; Secondary 54E52, 01A55

1 A Brief History of Transcendental Numbers

In mathematics, the notion of transcendence dates at least back to Gottfried Leibniz. According to Eberhard Knobloch [50], Leibniz had used the term *transcendental* since 1673 for different mathematical objects; in particular, the failure of algebraic methods to solve polynomial equations of degree five or higher led him to investigate

J. Steuding (✉)
Department of Mathematics, Würzburg University, Emil-Fischer-Str. 40, 97 074 Würzburg, Germany
e-mail: steuding@mathematik.uni-wuerzburg.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_29

the infinite by his differential calculus.[1] It was probably Leonhard Euler [29] in 1748 who was the first to provide a proper definition of a transcendental number. In modern terminology, a number ξ is called *transcendental* if it is not algebraic. Here a number ξ is said to be *algebraic* if there exists a not identically vanishing polynomial with integer coefficients having ξ as zero; the minimal degree of such a polynomial is said to be the degree of ξ. In 1844, Joseph Liouville [54–56] proved his famous approximation theorem for algebraic numbers: *for any algebraic number ξ of degree $d > 1$, there exists a positive constant c, depending only on ξ, such that*

$$\left|\xi - \frac{p}{q}\right| > \frac{c}{q^d}$$

for all rationals $\frac{p}{q}$ with $q > 0$.[2] Liouville's result has been significantly improved by Axel Thue, Freeman Dyson, Carl Ludwig Siegel, and, finally, Klaus Roth who succeeded in 1955 in showing that *for every algebraic ξ and every $\epsilon > 0$, there exist only finitely many rational solutions $\frac{p}{q}$ to the inequality*

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}},$$

independent of the degree of ξ. For this and further results of this flavour we refer to Hindry and Silverman [43].

Consequently, algebraic numbers cannot be approximated too good by rational numbers; moreover, numbers which allow better rational approximations are transcendental. This idea had been the motivation for Liouville for his studies on this topic in the period from 1840 to 1851; his main attempt to prove the transcendence of π or $e := \exp(1)$ failed, however, his approximation theorem had definitely influenced his protégé Charles Hermite [39] for his proof of the transcendence of e in 1873. In fact Hermite wrote[3]

> Dans cet ordre d'idées M. Liouville a déjà obtenu un théorème remarquable qui est l'objet de son travail intitulé: *Sur des classes très-étendus de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébrique*, et je rappellerai aussi que l'illustre géomètre a démontré le premier la proposition qui est le sujet de ces recherches pour les cas de l'équation du second degré et de l'équation bicarrée.

[1] Which he commented with his famous words "omnem rationem transcendunt".

[2] This final version appeared in [56]. His proof relies on an application of Rolle's theorem to the minimal polynomial of ξ.

[3] Hermite [39, p. 77]; English translation: "In this context, M. Liouville already obtained a remarkable theorem which is object of his work entitled: *Sur des classes très-étendus de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébrique*, and I also remind that the illustrious geometer was the first to show the proposition which is subject of this research for the case of an equation of second degree and of an equation of biquadratic degree".

Refining and extending Hermite's method, Ferdinand Lindemann[4] proved that also π is transcendental and, henceforth, the impossibility of squaring the circle by using only ruler and compass.

Liouville himself had been inspired by reading the correspondence between Christian Goldbach and Daniel Bernoulli published by Paul Heinrich von Fuss in 1843. As a matter of fact, Goldbach wrote in a letter from August 1729[5]:

> Here follows a series of fractions like the ones you have asked me for whose sum is neither rational nor the root of any rational number:

$$\frac{1}{10} + \frac{1}{100} + \frac{1}{10000} + \frac{1}{100000000} + etc \tag{1.1}$$

> The general term is $1/10^{2^{x-1}}$.

A proof of this statement is missing in their correspondence (and we shall say a few words about that in the final section). It is interesting that Liouville later confused Daniel Bernoulli with Euler when he reflected his very first attempts[6]:

> Je crois me souvenir qu'on trouve un théorème de ce genre, énoncé dans une lettre de Goldbach à Euler; mais je ne sache pas que la démonstration en ait jamais été donnée.

We shall have a closer look on Liouville's approach. A real number ξ is said to be a *Liouville number* if for every positive integer m there exist integers p_m and $q_m > 1$ such that

$$0 < \left| \xi - \frac{p_m}{q_m} \right| < \frac{1}{q_m^m}.$$

It is an immediate consequence of Liouville's theorem and the latter definition that *every Liouville number is transcendental.* The name is chosen well: Liouville gave first explicit examples of such numbers by the following regular continued fraction expansions

$$\xi = \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \cdots$$

[4] Who obtained his habilitation and venia legendi in 1877 at the University of Würzburg.

[5] cf. Lützen [57, p. 514].

[6] Liouville [56, p. 140]; English translation: "I think I can remember that one finds a theorem of this kind announced in a letter of Goldbach to Euler; however, I would not know whether its proof was ever given".

with partial quotients a_n recursively defined such that

$$\limsup_{n\to\infty} \frac{\log a_{n+1}}{\log q_n} = \infty, \tag{1.2}$$

where the q_n are the denominators of the convergents to ξ (see (4.1) below); for instance, setting $a_n = b^{n!}$ with an integer $b \geq 2$ provides such an expansion. Another class of examples that Liouville mentioned (without proof), which can still be found in many textbooks, is given by extremely fast converging infinite series as, for example,

$$\xi = \sum_{n\geq 1} \beta_n b^{-n!} \qquad \text{with arbitrary} \quad \beta_n \in \{0, 1, \dots, b-1\},$$

where again $b \geq 2$ is an integer. It therefore follows from Georg Cantor's famous diagonal argument that *there exist uncountably many Liouville numbers*.

Actually, when Cantor [15] started with his investigations on infinity in 1873, his focus was on algebraic numbers. His approach showed that (in modern language) *the set of algebraic numbers is countable and its complement, the set of transcendental numbers, is uncountable*; in fact, he wrote[7]

> (...) so fand ich den deutlichen Unterschied zwischen einem sogenannten Continuum und einem Inbegriffe der Art der Gesammtheit aller reellen algebraischen Zahlen.

This result came previous to Cantor's famous and slightly easier statement on the uncountability of the set of real numbers. Therefore, the beginning of set theory relies on Cantor's interest in number theoretical questions,[8] however, the story is more subtle. According to Dauben [20], Cantor's research of the early 1870s was devoted to the theory of trigonometric series and had a strong impact on his foundation of set theory; irrational numbers came into play with respect to exceptions of the convergence of a certain representation.

For more details on the history of Liouville's theorem we refer to Lützen's monograph [57]; for more details on transcendental numbers, see Burger and Tubbs [14] as well as Schneider's classic [70].[9]

[7] Cantor [15, p. 259]; English translation: "(...) so I found the significant difference between a so-called continuum and the epitome of all kind of real algebraic numbers."

[8] It might be interesting to notice that Cantor's doctorate entitled *De aequationibus secundi gradus indeterminatis* from 1867 dealed with quadratic forms and was supervised by Ernst Eduard Kummer.

[9] Which was one of Wolfgang Schwarz's favourite readings. Theodor Schneider was the thesis advisor of Wolfgang Schwarz; he is famous for solving the seventh Hilbert problem on the transcendence of α^β for algebraic β and $\alpha \neq 0, 1$ simultaneously with and independently to Aleksandar Gelfond in 1934.

2 The Papers by Erdős, Rieger, and Schwarz on Liouville Numbers

In 1962, Paul Erdős [27] proved that every real number is the sum (and product) of two Liouville numbers. His paper starts with the following words[10]:

> Some years ago I showed (possibly jointly with Mahler), that every real number is the sum of two Liouville numbers. A proof of the proposition may now be in the literature, but I do not know of any reference. In any case, the following slightly stronger theorem is now needed (see [1]), and therefore I publish a proof.

Actually, [1] is a paper by Melzak on the algebraic closure of plane sets, published as [61] the same year and in the same journal as Erdős' paper. Concerning the unclear statement of Erdős about the origin of his paper, there seems to be no reference in the literature before the publication of [27]. Erdős had been working with Kurt Mahler since the late 1930s.[11]

Here is Erdős' stronger theorem in its original form:

Theorem 2.1 (Erdős [27]) *To each real number* t $(t \neq 0)$ *there correspond Liouville numbers* x, y, u, v *such that*

$$t = x + y = uv.$$

Erdős' gave a *constructive* elementary proof (using the binary expansion of real numbers) and another *non-constructive* one using a category argument which[12]

> may be of interest because of its generality. The set L of Liouville numbers, being a dense set of type G_δ, is residual (in other words, it is the complement of a set of first category). Let A and B be any two residual sets of real numbers. For each real number t, the set B_t of numbers $t-b$ $(b \in B)$ is also residual, and therefore it contains a point x of A. Let $y = t-x$. Then $y \in B$, and since $t = x + y$, we have shown that each real number is the sum of a number in A and a number in B. We now obtain the first part of the theorem by choosing $A = B = L$.

Obviously, the categorial reasoning holds for much more general sets. Notice that the complements of A and B_t are both of first category, i.e., they are countable unions of nowhere dense sets,[13]

$$\mathbb{R} \setminus A = \bigcup_n M_n, \qquad \mathbb{R} \setminus B_t = \bigcup_m N_m.$$

[10] Erdős [27, p. 59].

[11] As indicated by his warm-hearted obituary [28].

[12] Erdős [27, p. 60].

[13] A set M is said to be *dense* in a topological space X if every point of X is either an element of M or a limit point of M; a set is called *nowhere dense* if its closure has no interior points.

Hence,

$$A \cap B_t = \bigcap_n (\mathbb{R} \setminus M_n) \cap \bigcap_m (\mathbb{R} \setminus N_m)$$

is dense by Baire's theorem and therefore not empty. We shall focus here on the additive representation and restate Erdős' observation in a more general form:

Theorem 2.2 (Erdős' Theorem, Categorial Version) *Let $A, B \subset \mathbb{R}$ be residual, then*

$$\mathbb{R} = A + B.$$

Here $A + B$ is the so-called Minkowski sum defined as $\{a + b : a \in A, b \in B\}$.

For the sake of completeness we shall briefly recall basic notions from topology and category theory.[14]

Theorem 2.3 (Baire's Theorem [5]) *Any countable intersection of dense open subsets (of a complete metric space) is dense. Equivalently, the complement of a meagre set is dense.*

A set $M \subset \mathbb{R}$ is said to be of *first category* or *meagre* if it is a countable union of nowhere dense sets; otherwise, M is said to be of *second category* (or *comeagre*). The complement of a set of first category is called *residual*. By Baire's theorem, every residual set is dense. A subset G is called a G_δ*-set* if it is a countable intersection of open sets. Consequently, the countable intersection of dense G_δ-sets is a dense G_δ-set and every residual set is dense.

In particular, this implies that the set

$$L := (\mathbb{R} \setminus \mathbb{Q}) \cap \bigcap_{n \geq 1} \left(\bigcup_{q \geq 2} \bigcup_p \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right) \right)$$

of Liouville numbers is a residual and dense G_δ-set. It is remarkable that L is big in the sense of category and small in the sense of measure (having Hausdorff and Lebesgue measure zero). For the set of normal numbers to all bases it is the other way around and this is attributed to Émile Borel [10] (concerning the measure theoretical statement)[15] and Lars Olsen [63] (proving the categorial part).

[14] A very recommendable monograph on this topic is the book by Oxtoby [67] studying both subjects simultaneously.

[15] Actually, Borel's original proof of the statement that *almost all real numbers are normal to any base* (in the sense of Lebesgue measure) was based on a strong law of large numbers and faulty; it has been corrected by Cantelli and is now known as the Borel–Cantelli lemma. The first rigorous proof of Borel's statement about normal numbers is due to Georg Faber [30] and Felix Hausdorff [38], respectively. We refer to Barone and Novikoff [8] for details about the interesting polemic between Borel and Cantor's pupil Felix Bernstein.

It seems that Erdős' interest in category theory started with his article [26] from 1943 in which he refined a result by Wacław Sierpiński [75] by showing, under assumption of the continuum hypothesis, the existence of an involution $f : \mathbb{R} \to \mathbb{R}$ for which $f(M)$ has measure zero if and only if M is of first category.[16]

In 1975, Georg Johann Rieger [68] generalized Erdős' result on Liouville numbers by proving

Theorem 2.4 (Rieger [68]) *Suppose that $f_1, \ldots, f_r$ are real-valued continuous and strictly increasing functions defined on the closed unit interval; then there exist uncountably many Liouville numbers ξ in the open unit interval such that $f_1(\xi), \ldots, f_r(\xi)$ are Liouville numbers too.*

His reasoning is elementary, the case $r = 1$ is constructive. Taking the functions $t \mapsto f(t) = \xi - t$, resp. $f(t) = \xi/t$, yields Erdős' Theorem 2.1. Furthermore, Rieger investigated the solvability of systems of real linear equations in Liouville numbers and proved that for every real $t > 1$ there exist Liouville numbers α, β such that $t = \alpha^\beta$.

In 1977, Wolfgang Schwarz [71] gave another and in some sense final generalization of both, Erdős' and Rieger's result by showing

Theorem 2.5 (Schwarz [71]) *Given (at most) countably many continuous open mappings $f_r : (0,1) \to \mathbb{R}$, $r = 1, 2, \ldots$, there exists a dense G_δ-subset D of $(0,1)$ consisting only of Liouville numbers ξ such that all $f_r(\xi)$, $r = 1, 2, \ldots$ are again Liouville numbers.*

The non-constructive proof is inspired by the works of Erdős and Rieger and relies once again on Baire's theorem. The paper is very short, just three pages (and this is also approximately the number of pages of the preceding papers of Erdős and Rieger). Here is Schwarz's elegant

Proof The set L of Liouville numbers is a dense G_δ-set. The same is true for the intersection with $B_r := f_r((0,1))$. In view of the continuity the pre-images $A_r := f_r^{-1}(L \cap B_r)$ are also G_δ-sets, and because of f_n being open and surjective, they are dense in $(0,1)$ as well. Thus, by Baire's theorem, the countable intersection

$$D = (L \cap (0,1)) \cap \bigcap_r A_r$$

is again a dense G_δ-set (and in particular uncountable); it follows from

$$f_r(D) \subset f_r(A_r) \subset f_r(f_r^{-1}(L \cap B_r)) \subset L \cap B_r$$

that $f_r(\xi) \in L$ for every $\xi \in D$. This proves the assertion.

[16] See Oxtoby's textbook [67, Chap. 19], for further details.

There are a few articles extending and generalizing the results of Erdős, Rieger, and Schwarz. We do not intend to give a complete list of those papers but mention Kamil Alniaçik and Eric Saias [1] who showed that *if $I \subset \mathbb{R}$ is an interval with non-empty interior, G a G_δ-subset of $\mathbb{R}$, and (f_n) a sequence of continuous and nowhere locally constant mappings $f_n : I \to \mathbb{R}$, then $\bigcap_n f_n^{-1}(G)$ is a G_δ-subset of I*. Edward Burger [13] gave an analogue for local fields. Senthil Kumar et al. [73] investigated questions around the algebraic independence of Liouville numbers and Schanuel's conjecture in the framework of G_δ-sets.

Applications of functional analysis to number theory were one of the major themes in the research of Wolfgang Schwarz. Besides the example from above there should be mentioned the application of Gelfand theory of commutative Banach algebras to arithmetical functions; see [46] for an overview.

3 A Brief History of Baire's Theorem and Related Topics

Building on concepts and definitions established by Cantor and Paul du Bois-Reymond in the course of foundation of set theory and analysis, René-Louis Baire proved in his thesis from 1899 his famous category theorem. In modern language this statement can be formulated as follows:

Theorem 3.1 (Baire's Theorem, Modern Version) *If X is a complete metric space and S a countable union of nowhere dense sets in X, then the complement of S is dense in X.*

A space is said to be *Baire* if each countable intersection of dense open subsets is dense. Hence, Baire's theorem implies that all completely metrizable spaces and all compact Hausdorff spaces are Baire.

It took about 20 years that Baire's theorem was extended to other complete metric spaces. Nowadays Baire's theorem is interpreted as the origin for three major results in functional analysis, namely the *uniform boundedness principle* (first proved by Stanisław Saks 1929 building on previous work of Henri Lebesgue 1909), the *open mapping theorem* (due to Stefan Banach and Juliusz Schauder 1929), and the *closed graph theorem*. A typical corollary is, for instance, due to Banach [6] and Stefan Mazurkiewicz [60] who deduced in 1931 from Baire's theorem that *the generic continuous function on an arbitrary compact interval is not monotone on any subinterval and nowhere differentiable.*[17] In fact, Baire's approach often allows to prove the existence of a function with certain counter-intuitive properties as, for example, the Weierstrass' monsters of nowhere differentiable continuous functions, whereas the explicit construction might be difficult.[18]

[17] Building on previous work by Hugo Steinhaus [78].

[18] See Volkert [82] for a historical discussion of Weierstrass' construction and its generalization.

We shall have a closer look on the origin of Baire's work. As a matter of fact, Baire's theorem is just a more precise formulation of Cantor's observation on the uncountability of the real numbers, and indeed Cantor's first proof of this statement is built on essentially the same ideas which are used to prove Baire's category theorem. Therefore, we shall also take Cantor into account and indicate how his work inspired Baire.

Much has been written about Cantor's path-breaking foundation of set theory in the 1870s. Mathematics and mathematical thinking at his time was rather different from what they are today. In particular, the notion of infinity was used in an imprecise way and infinite sets were considered countable (to use modern language). Carl Friedrich Gauß wrote in a letter to his friend Heinrich Christian Schumacher[19]:

> (...) so protestiere ich (...) gegen den Gebrauch einer unendlichen Grösse als einer Vollendeten, welcher in der Mathematik niemals erlaubt ist. Das Unendliche ist nur eine façon de parler.

It is indeed the new concept of infinity which stands at the beginning of Cantor's work and Baire's theorem. Pierre Dugac wrote about Baire[20]:

> D'ailleurs, ce sera BAIRE qui utilisera pour la première fois en France, de façon systématique, les travaux de GEORG CANTOR, aussi bien ceux concernant la topologie générale que ceux traitant du transfini. A. DENJOY nous disait que 'ça ne fait pas de doute', et que 'l'influence de CANTOR sur RENÉ BAIRE a été considérable'. En particulier, c'est par le transfini 'que Cantor est continuellement présent dans l'oeuvre de Baire'. Par contre, 'jamais Baire n'a fait appel à l'hypothèse que les nombres réels forment un ensemble bien ordonné. Il s'est toujour tenu au dénombrable

And Oliver Deiser wrote[21]:

> Die nirgends dichte Cantormenge hatte Cantor bereits 1883 betrachtet, weiter kann man seinen ersten brieflich mit Dedekind diskutierten Beweis der Überabzählbarkeit von $\mathbb{R}$ als einen Beweis des Kategoriensatzes lesen. Aber erst Baire hat die Begriffe klar herausgestellt.

[19] cf. Ilgauds and Purkert [45, p. 47], resp. Maor [59, p. 55]; English translation: "(...) so I protest against using an infinite quantity as accomplished which is nowhere allowed in mathematics. The infinite is only a façon de parler." Here the word 'façon de parler' can be translated literally as 'manner of speaking'.

[20] Dugac [23, p. 317]; English translation: "By the way, there is BAIRE who was the first in France to use GEORG CANTOR's works in a systematic way in exactly the general topology of infinity. A. DENJOY told us that 'there is no doubt' and that 'CANTOR's influence on RENÉ BAIRE was substantial'. In particular when it is about infinity 'Cantor is present in Baire's work'. On the contrary 'Baire himself never appealed to the hypothesis that the real numbers form a well-ordered set. He always believed them to be countable".

[21] Deiser [21, p. 494]; English translation: "The nowhere dense ([middle third] Cantor set had already been considered by Cantor in 1883, moreover, one can read his proof of the uncountability of $\mathbb{R}$, first discussed with Dedekind in a letter, as a proof of the category theorem. However, it was Baire to emphasize the concept".

A historical comment is in order. It was Henry John Stephen Smith [77] who was the first to study the middle third Cantor set[22] in 1874, almost 10 years before Cantor [16], Vito Volterra [83] in 1881, and du Bois-Reymond [22] in 1880.[23]

In order to indicate the very origin of Baire's theorem we shall sketch the proof of Baire's theorem (in the shape of Theorem 2.3 for $\mathbb{R}$) in a nutshell: Given dense open subsets $D_1, D_2, \ldots$ of $\mathbb{R}$, also $\bigcap_{1\le n\le m} D_n$ is open and dense. Let $\{J_k\}$ be an enumeration of rational intervals and let $I_0 \neq \emptyset$ be an arbitrary open interval. Define $I_{n+1} = J_k = (\ell_k, r_k)$, where k is the least positive integer such that $[\ell_k, r_k] \subset I_n \cap D_n$. It follows that

$$\ell := \lim_{k\to\infty} \ell_k \in I \cap \left(\bigcap_{n\ge 1} D_n \right),$$

which shows that the intersection of countably many open sets is dense in $\mathbb{R}$.

Indeed, Cantor wrote to Richard Dedekind in a letter from December 1873[24]:

> Es lässt sich nun stets wenigstens eine Zahl, ich will sie η nennen, denken, welche im Innern eines jeden dieser Intervalle liegt; von dieser Zahl η (...) sieht man rasch, daß sie in keiner unserer Reihen (...) enthalten sein kann. (...) folglich ist die Voraussetzung eine unrichtige gewesen.

The proof with the famous diagonal argument was given by Cantor much later, namely in 1890 and appeared in the first issue of the journal of the just founded *Deutschen Mathematiker Vereinigung*[25] [18].

In the beginning, when René-Louis Baire [5] proved a first version of his famous theorem, it was a statement about the set of discontinuities of a function of several variables which is continuous with respect to each variable separately. Baire succeeded to prove that such (not necessarily) continuous functions are pointwise discontinuous on each perfect set. In fact, Baire's theorem explains how infinitely real differentiable functions differ from analytic functions. However, already in 1896, William Osgood [64, 65] obtained the statement for functions of one variable. About Baire's contribution Edward B. van Vleck wrote[26]:

> BAIRE in his important thesis has given a number of interesting theorems concerning pointwise discontinuous functions. For their demonstration he employs the concept of semi- (i.e., upper or lower) continuity. However necessary the concept may be found for

[22] Which is constructed by removing each middle third of the unit interval and all remaining intervals.

[23] For this and the rather difficult relation between the latter mathematician and Cantor see Laugwitz [53].

[24] Cavaillès and Noether [19]; English translation: "Now we can think of a number, I will call it η, which lies in the interior of all these intervals; it follows easily that this number η is not contained in any of our sequences, henceforth our assumptions was false".

[25] German Mathematicians Association; Cantor was one of the founders of this society in 1890.

[26] van Vleck [79, p. 189]; in the original the names of Osgood and Baire are written in small capitals as well.

> subsequent portions of his investigation, its introduction is not needed for the particular theorems referred to. When the unnecessary element is removed, the principles of their demonstration, although very different in form, become equivalent to those used by OSGOOD in the derivation of his theorem relating to the convergence of series of continuous functions. (...) It is found that BAIRE has restricted $f(x, y)$ more than is necessary in the following theorem: (...)

Osgood and van Vleck were at that time two of the many young and talented U.S. American mathematicians studying at well-established European universities[27] and later founding a strong American school of analysis. Osgood [66] was the first to prove the Riemann mapping theorem in its full generality (for simply connected domains with arbitrary boundaries). And van Vleck [80] was very close to prove the Borel attributed theorem that almost all real numbers are normal, mentioned above. There he also established a first zero-one law previous to the attempts of Borel, Cantelli, and others.[28] The following stupid words should not be hidden in a footnote: during World War I van Vleck wrote about the Lebesgue integral that[29]

> This new integral is proving itself a wonderful tool. I might compare it to a modern Krupp gun, so easily does it penetrate barriers which before were impregnable.

Actually, van Vleck was rather influential, serving as an editor of the Transactions of the American Mathematical Society from 1905 to 1910, as vice-president in 1909, and, finally, president in the years 1913 and 1914.

We return to Baire's theorem. Interestingly, there had been another forerunner apart from Osgood. As early as 1884 Ludwig Scheeffer used a similar reasoning in his discussion of continuous functions. In his article [69] he proved among other things the following remarkable *Hülfssatz aus der Mengenlehre*[30]:

> Es sei P eine beliebige perfekte Menge, welche in keinem Intervall überall dicht ist, R eine beliebige abzählbare Menge. Subtrahirt man von allen Elementen der Menge P eine Konstante a, so entsteht eine aus den Werten $x - a$ gebildete neue Menge P_a. Es lässt sich dann die Konstante a zwischen beliebig gegebenen Grenzen immer so bestimmen, dass die Menge P_a keinen einzigen Wert von der Menge R enthält.

In modern language this means that *if R is a countable set of real numbers and $P \subset \mathbb{R}$ is nowhere dense, then there exists an everywhere dense set A such that $R + a \cap P$ is empty* (where $R + a := \{r + a \,:\, r \in R\}$).

Scheeffer's result has been extended by Frederick Bagemihl [2] who showed that the statement of the *Hülfssatz* is even true if P is of first category, i.e., *if R is countable and P is of first category, then there exists a residual set A such that*

[27] In the case of Osgood and van Vleck both studied and worked with Felix Klein in Göttingen.

[28] See Barone and Novikoff [7] for details.

[29] van Vleck [81, p. 7].

[30] Scheeffer [69, p. 291]; English translation: "Let P be an arbitrary perfect set which is not dense in any interval, and R an arbitrary countable set. Subtracting a constant a from all elements of P, the values $x - a$ form a new set P_a. Then one can always determine the constant a in between given bounds such that the set P_a contains no value from the set R". The word '*Hülfssatz*' is old-fashioned German for a proposition.

$R + a \cap P$ *is empty for every* $a \in A$. The proof reminds us on Erdős' reasoning in his categorial proof of Theorem 2.1.[31] This observation may be used to prove, for example, the existence of real numbers r such that translates of the middle third Cantor set by r, $\mathcal{C} + r$, are disjoint with the set of rational numbers; notice that $\mathcal{C}$ is of first category.[32]

Scheeffer was a pupil of Cantor who also wrote an obituary [17] on him after his untimely death in 1885 caused by typhus; there one can read about Scheeffer's work[33]:

> Eine gründliche Gelehrsamkeit, verbunden mit Reichtum an eigenen Gedanken, welche mit musterhafter Einfachheit, Klarheit und Eleganz der Sprache zur Darstellung kommen, bildet das wesentliche Merkmal seiner Produktionen. Von den schönen Resultaten, zu welchen ihn seine mit ei–sernem Fleiß gepflogenen Untersuchungen geführt haben, möge hier der in Nr. 4 gelieferte Beweis für den folgenden Satz hervorgehoben werden:
> "Wenn man von einer stetigen Funktion einer Veränderlichen weiß, daß ihr Differentialquotient Null ist für alle Werte eines Intervalls, mit *Ausnahme derjenigen, welche irgendeiner gegebenen unendlichen Punktmenge erster Mächtigkeit entsprechen*, so folgt hieraus, daß die Funktion in dem gedachten Intervall eine Konstante ist."

This theorem reminds us strongly of results obtained by the Polish school of functional analysts around Banach mentioned in the beginning of this section. Such results are indeed typical for applications of Baire's theorem or, to include Scheeffer's statement, categorial reasoning built on Cantor's set theory. The notion '*erste Mächtigkeit*' characterizes here a discrete set of real numbers, a concept introduced by Axel Harnack [36] to relate point-sets with intervals that has been driven further by Borel and others, being the backbone of Lebesgue theory.[34]

[31] It is remarkable that Bagemihl's paper [2] was published in the same journal as Erdős' article [27] on Liouville numbers about a decade earlier; it might be even more remarkable that in this second issue of the *Michigan Mathematical Journal* there is a paper by Gerald Mac Lane [58] on a conjecture by Erdős and others published on the previous pages. However, taking more than 1500 publications of Erdős and their deep impact into account this might have no meaning at all. Scheeffer's theorem is also mentioned in the at that time rather influential monograph [76] by Sierpiński.

[32] The author has learned about Scheeffer's work and all the other details mentioned above by the blog *mathoverflow* and the valuable comments of Andres Caicedo on the question entitled 'A translation of the Cantor set contained in the irrationals', posted February 22, 2014, and based on Wilman Brito's book [11].

[33] Cantor [17, p. 199]; engl. translation: "A sound scholarliness connected with plenty of own thoughts, which with exemplary simplicity, clearness, and elegant language are constituted, are the essential character of his productions. Of his beautiful results, to which he was guided by his brassbound diligence driven investigations, I would like to accent here the proof of the following theorem from No. 4:

"If one knows about a continuous function of one variable that its differential quotient is zero for all values of an interval with *exception of those which constitute an arbitrarily given infinite set of first cardinality*, then the function is a constant in this interval."" The words in *italics* are also in the original in italics.

[34] Scheeffer [69] uses with 'Inhalt Null' (meaning 'content zero') another notion introduced by Cantor in place of 'erster Mächtigkeit'.

The paper in question, Nr. 4 in Cantor's list of Scheeffer's publications, is [69], mentioned above containing the forerunner of Baire's theorem.

Actually, Baire was aware of Scheeffer's work. In a letter to Volterra, dated March 8, 1899, Baire wrote about an article by Dmitry Gravé [32] that[35]:

> Sa note ne me semble pas très originale, car l'exemple qui'il donne n'est pas autre chose qu'un exemple donné en 1885 par Ludwig Scheeffer dans un mémoire des Acta Mathematica (Tome V), et auquel, d'ailleurs, je renvoie dans le dernier chapitre de ma thése. L'exposition seule diffère, et je me demande s'il peut y avoir là une simple coïncidence. Cette note a été présentée par M. Picard, à son retour de voyage; je mais proposais de lui en dire un mot, mais j'ai complétement oublié à la dernière visite que je lui ai faite; je lui en parlerai une autre fois.

The thesis mentioned here is, of course, Baire's thesis, later published as [5], and the mathematician behind *M. Picard* is, of course, Monsieur Émile Picard.

There is another episode to be told in this context, namely the aspect of constructive proofs and a related dispute. It is well known that Cantor's former promoter Leopold Kronecker became a strong opponent to Cantor's modern set theory; his famous words[36]

> Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

give proof of his clear position in favour of constructive methods and against infinite constructions. It was the young generation of mathematicians who cherished Cantor's foundation of modern set theory; for instance, David Hilbert who wrote[37]:

> Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können.

Moreover, at the very first International Congress for Mathematicians, held at Zurich in 1897, Adolf Hurwitz [44] gave a talk on recent developments in complex analysis and the impact of Cantor's set theory.

A rather explicit example of the two contrary positions of Cantor and Kronecker seems to give different proofs of the existence of transcendental numbers. Whereas Liouville's proof is constructive Cantor's reasoning is different, at least on first glimpse non-constructive and therefore inacceptable by Kronecker and his fellows. It was first observed by Israel Nathan Herstein and Irving Kaplansky [41] in 1974 that contrary to that what is written in many textbooks Cantor's diagonal argument

[35]Dugac [23, p. 349]; English translation: "His note does not seem to be very original, in particular since his example had been given 1885 by Ludwig Scheeffer in his treatise in Acta Mathematica (Tome V), and to which I refer to in the last chapter of my thesis. Only the presentation differs and I ask myself whether there could have been a simple coincidence. The note had been communicated by M. Picard after the return from his journey; I could offer to talk to him, however, I had completely forgotten at my last visit; I could talk to him about that another time." In the author's opinion there are different interpretations of the notion 'je me demande s'il peut y avoir là une simple coïncidence'. possible here.

[36]cf. Weber [84, p. 15]; English translation: "God made natural numbers, all else is the work of man".

[37]Hilbert [42, p. 170]; English translation: "No one shall expel us from the paradise that Cantor has created".

is in some sense constructive, and it was Richard Gray [33] who computed by a detailed analysis the complexity with which 'Cantor's methods lead to computer programs that generate transcendentals'. Nevertheless, we observe a difference with respect to representability in the examples of transcendental numbers provided by Liouville's method versus the reasoning of Cantor and Gray. Note that Erdős' reasoning for Theorem 2.1 based on Baire's theorem is obviously just an existence proof and not constructive.

In 1904, Ernst Zermelo [85][38] introduced the axiom of choice **AC** in order to prove Cantor's conjecture on the well-ordering of arbitrary sets for which Zermelo is sometimes considered as the true founder of abstract set theory.[39] Often **AC** plays a substantial role in proving that a space is Baire. However, sometimes a weaker version of **AC** is sufficient, e.g., the *principle of dependent choices* **DC** which states that, for every pair (X, ρ), where X is a non-empty set and ρ is a relation on X such that for all $x \in X$ there is some $y \in X$ such that $x \rho y$, there exists a sequence (x_n) in X with $x_n \rho x_{n+1}$ for each n. One can show that **DC** is equivalent to compact Hausdorff spaces being Baire (as was shown by Charles E. Blair [9]).

Baire and contemporary French analysts were not against non-constructive proofs or Cantor's set theory, in the discussion about **AC**, however, they turned out to be rather conservative; according to Akihiro Kanamori [48][40]:

> Baire [1899:36] viewed the infinite ordinal numbers and hence his function hierarchy as merely *une façon de parler*, and continued to view infinite concepts only in potentiality. Borel [1898] took a pragmatic approach and seemed to accept the countable ordinal numbers. Lebesgue was more equi–vocal but still accepting; recalling Cantor's early attitude Lebesgue regarded the ordinal numbers as an indexing system, "symbols" for classes, but nontheless he worked out their basic properties, even providing a formulation [1905:149] of proof by transfinite induction. All three analysts expressed misgivings about AC and its use in Zermelo's proof.

Indeed, from a modern point of view their aloofness to abstract set theory is surprising and may be even considered ironic with respect to their contributions and what grew out of them.[41] In particular Baire expressed his disapproving position with respect to **AC** with a drastic racist statement[42]:

> It is surprising that it is the Germanic races, with a heavy and correct spirit, that throw up these rash assertions; it would perhaps be more comprehensible among the hare-brained Latins.

[38] It might be interesting to notice that his article has the subtitle "Aus einem an Herrn Hilbert gerichteten Briefe", and that he wrote further "Die Idee (...) verdanke ich Herrn Erhard Schmidt". meaning that the article contains material from a letter written to Hilbert and that the idea behind is due to Schmidt.

[39] "Hence, Zermelo rather than Cantor should be regarded as the creator of abstract set theory" wrote Kanamori [48, p. 15].

[40] The appearing brackets point to publications of the three authors indicating the year and page.

[41] For a change of thinking credit should be given to, among others, Hausdorff and the Polish school of functional analysts.

[42] cf. Gray [34, p. 258].

For more details about Baire's life, his uneasy character and the quarrels with Henri Lebesgue and Charles de la Vallée Poussin as well as an overview on the various applications of Baire's theorem we refer to Dugac [23] and Jones [47]. A good reading about Cantor's life and work is the monography of Ilgauds and Purkert [45] and we refer to Gispert [31] for details about the reception of Cantor's set theory in France. The history of the axiom of choice and its mathematical impact has been treated by Moore [62] and more recently by Herrlich [40].

4 Imposing Residue Class Constraints: New Results

Given positive integers $a \le b, c \le d$, we say that an irrational real number ξ is a *restricted Liouville number with respect to the pair of residue classes* $(a \bmod b, c \bmod d)$ if for infinitely many positive integers m there exist pairs of integers $(p_m, q_m) \in (a \bmod b, c \bmod d)$ with positive q_m such that

$$\left|\xi - \frac{p_m}{q_m}\right| < \frac{1}{q_m^m};$$

we denote by $L(\frac{a \bmod b}{c \bmod d})$ the set of all such restricted Liouville numbers ξ.

Theorem 4.1 *For every choice of positive integers a, b, c, d with coprime a and c the set $L(\frac{a \bmod b}{c \bmod d})$ is an uncountable subset of L.*

Proof We may assume that $b, d \ge 2$. We expand $\frac{a}{c}$ into a finite regular continued fraction

$$\frac{a}{c} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_m}}} =: [a_0, a_1, \ldots, a_m]$$

with positive integer partial quotients a_n. We shall extend this expansion by continuing this fraction further. Recall the recursion formulae for continued fractions,

$$\begin{cases} p_{-1} = 1,\ p_0 = a_0 & \text{and} \quad p_n = a_n p_{n-1} + p_{n-2}, \\ q_{-1} = 0,\ q_0 = 1 & \text{and} \quad q_n = a_n q_{n-1} + q_{n-2}. \end{cases} \qquad (n \in \mathbb{N}) \qquad (4.1)$$

In view of the coprimality we have $p_m = a$ and $q_m = c$. Let $a_n = \ell^{\delta(n)}$ with $\ell := \operatorname{lcm}[b, d]$ for all indices $n > m$ satisfying $n \equiv m \bmod 2$ and a strictly increasing integer-valued arithmetical function $\delta : \mathbb{N} \to \mathbb{N}$. Then, we obtain by induction

$$p_{m+2k} = a_{m+2k} p_{m+2k-1} + p_{m+2(k-1)} \equiv a \bmod b,$$
$$q_{m+2k} = a_{m+2k} q_{m+2k-1} + q_{m+2(k-1)} \equiv c \bmod d$$

for $k \in \mathbb{N}$. So far there is no constraint on the partial quotients a_n with index $n > m$ if $n \not\equiv m \bmod 2$. Assigning arbitrary positive integer values to the partial quotients a_n for these indices n, we may define real numbers by the corresponding continued fraction expansion

$$\xi := \xi(\mathfrak{a}, \delta) = [\lfloor \xi \rfloor, a_1, \dots, a_m, a_{m+1}, \dots, a_n, \dots];$$

We notice that, by construction, every second convergent meets the residue class conditions.

Next we shall specify the arithmetical function δ in such a way that ξ is a Liouville number. For this purpose recall the classical estimate

$$\left| \xi - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1} q_n^2}.$$

Hence, ξ is a Liouville number if for all

$$q_n^{n-2} < a_{n+1} = \ell^{\delta(n+1)} \qquad \text{for all} \quad n > m,\ n+1 \equiv m \bmod 2. \tag{4.2}$$

In fact, we define $\delta(n+1)$ inductively such that this inequality is satisfied as Liouville did with (1.2). For the remaining partial quotients $a_{m+1}, a_{m+3}, \dots$ we allow arbitrary positive integers less than d, and call them the *digits* of ξ and write $\xi = \xi(a_{m+1}, a_{m+3}, \dots)$. We thus have shown that ξ is a Liouville number in $L(\frac{a \bmod b}{c \bmod d})$.

It remains to show that $L(\frac{a \bmod b}{c \bmod d})$ is uncountable. For this purpose we assume that the set of all restricted Liouville numbers

$$\xi(a_{m+1}, a_{m+3}, \dots, a_{m+2k+1}, \dots) \qquad \text{with} \quad a_{m+2k+1} \in \{0, 1, \dots, d-1\}$$

from the construction above (with fixed $a_1, \dots, \dots, a_m$ and δ) is countable and

$$\xi_n := \xi(a_{m+1}^{(n)}, a_{m+3}^{(n)}, \dots, a_{m+2k+1}^{(n)}, \dots) \qquad \text{for} \quad n = 1, 2, \dots$$

is a list of those. Define

$$\xi = \xi(b_{m+1}, b_{m+3}, \dots, b_{m+2k+1}, \dots) \qquad \text{with} \quad b_{m+2k+1} = \begin{cases} 1 \text{ if } \quad a_{m+2k+1}^{(k)} \neq 1, \\ 0 \text{ otherwise.} \end{cases}$$

In view of this choice, we obtain $\xi \neq \xi_k$ for any $k \in \mathbb{N}$ which shows that already the set of all $\xi(a_{m+1}, a_{m+3}, \dots, a_{m+2k+1}, \dots)$ is uncountable. The theorem is proved.

Our next aim is to prove the analogue of Erdős' Theorem 2.1 for restricted Liouville numbers. However, for this purpose we shall consider infinite series in place of continued fractions.

Theorem 4.2 *Assume that b and c are both coprime with d. Then, for every real number t there exist restricted Liouville numbers $\xi_1, \xi_2 \in L(\frac{a \bmod b}{c \bmod d})$ such that*

$$t = \xi_1 + \xi_2.$$

Proof By assumption, there exists a non-negative integer e such that $b^e \equiv c \bmod d$. Let $B = b^{\varphi(d)}$, where φ is Euler's totient. For a given ρ we consider the B-adic expansion of tb^e, i.e.,

$$tb^e = \gamma_0 + \sum_{n \geq 1} \gamma_n B^{-n} \qquad \text{with} \quad \gamma_0 \in \mathbb{Z},\ \gamma_n \in \{0, 1, \ldots, B-1\}.$$

It is easy to see that with ξ also $\pm\xi + z$ with integer z is a restricted Liouville number from $L(\frac{a \bmod b}{c \bmod d})$. Therefore, we may suppose that γ_0 is zero. For $j = 1, 2$, we define

$$\xi_j = \sum_{n \geq 1} \beta_n^{(j)} B^{-n} b^{-e}$$

by assigning digits $\beta_n^{(j)}$ as follows: for $k! < n < (k+1)!$,

$$\beta_n^{(1)} = \gamma_n,\ \beta_n^{(2)} = 0 \qquad \text{if} \quad k \equiv 1 \bmod 2,$$

and

$$\beta_n^{(1)} = 0,\ \beta_n^{(2)} = \gamma_n \qquad \text{if} \quad k \equiv 0 \bmod 2;$$

moreover, we let

$$\beta_{k!}^{(1)} = a,\ \beta_{k!}^{(2)} = \gamma_{k!} - a \qquad \text{if} \quad k \equiv 1 \bmod 2,$$

and

$$\beta_{k!}^{(1)} = \gamma_{k!} - a,\ \beta_{k!}^{(2)} = a \qquad \text{if} \quad k \equiv 0 \bmod 2.$$

Consequently, $\beta_n^{(1)} + \beta_n^{(2)} = \gamma_n$ for all n and $t = \xi_1 + \xi_2$. It remains to show that $\xi_j \in L(\frac{a \bmod b}{c \bmod d})$.

For $j = 1, 2$, put $q_m^{(j)} = B^{(m+1)!} b^e$ and

$$p_m^{(j)} = q_m^{(j)} \sum_{n \leq (m+1)!} \beta_n^{(j)} B^{-n} b^{-e} = \sum_{n \leq (m+1)!} \beta_n^{(j)} B^{(m+1)!-n}.$$

Consequently, $q_m^{(j)} \equiv c \bmod d$ and $p_m^{(j)} \equiv \beta_{(m+1)!}^{(j)} \equiv a \bmod b$. Hence, the residue conditions are fulfilled. Furthermore, it follows that

$$0 < \xi_j - \frac{p_m^{(j)}}{q_m^{(j)}} = \sum_{n>(m+1)!} \beta_n^{(j)} B^{-n} b^{-e}.$$

In view of the construction the series on the right-hand side has vanishing digits for $n \le (m+2)!$ whenever $m \equiv j \bmod 2$ which yields the upper bound

$$\sum_{n>(m+2)!} \beta_n^{(j)} B^{-n} b^{-e} < B^{-(m+2)!} b^{-e} = \frac{b^{e(m-1)}}{B^{2\cdot(m+1)!}} \frac{1}{(q_m^{(j)})^m} < \frac{1}{(q_m^{(j)})^m}.$$

The theorem is proved.

Our next and final aim is to prove stronger statements by use of Baire's theorem. It is remarkable how easy the categorial method leads to stronger results than the just given constructive approach.

First of all, we derive from the definition of restricted Liouville numbers the following representation as

$$L(\tfrac{a \bmod b}{c \bmod d}) = (\mathbb{R} \setminus \mathbb{Q}) \cap \bigcap_{n\ge 1} \left(\bigcup_{\substack{q\ge 2 \\ q\equiv c \bmod d}} \bigcup_{\substack{p \\ p\equiv a \bmod b}} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right) \right).$$

Thus, $L(\frac{a \bmod b}{c \bmod d})$ *is residual and a* G_δ*-set.* It is not difficult to show that the image of

$$f : \mathbb{N} \times \mathbb{N} \qquad (x, y) \mapsto \frac{a + bx}{c + dy}$$

is dense in $\mathbb{R}_{\ge 0}$. Hence, it follows that also $L(\frac{a \bmod b}{c \bmod d})$ is dense in $\mathbb{R}$ (without any assumption on a, b, c, d). Consequently, by Erdős' Theorem 2.2, we obtain

Corollary 4.3 *For any choice of positive integers* $a_j \le b_j, c_j \le d_j$ $(j = 1, 2)$,

$$\mathbb{R} = L(\tfrac{a_1 \bmod b_1}{c_1 \bmod d_1}) + L(\tfrac{a_2 \bmod b_2}{c_2 \bmod d_2})$$

Finally, we shall prove an analogue of Wolfgang Schwarz's Theorem 2.5 for restricted Liouville numbers:

Theorem 4.4 *Given positive integers* $a \le b, c \le d$*, (at most) countably many continuous open mappings* $f_r : (0, 1) \to \mathbb{R}$*, and sets of restricted Liouville numbers* $L(\frac{a_r \bmod b_r}{c_r \bmod d_r})$ *for* $r = 1, 2, \ldots$*, there exists a dense* G_δ*-subset* D *of* $(0, 1)$ *consisting only of restricted Liouville numbers* $\xi \in L(\frac{a \bmod b}{c \bmod d})$ *such that all* $f_r(\xi)$ *are restricted Liouville numbers from* $L(\frac{a_r \bmod b_r}{c_r \bmod d_r})$ *for* $r = 1, 2, \ldots$.

Proof (along the lines of Schwarz's reasoning) Every set $L(\frac{a_r \bmod b_r}{c_r \bmod d_r})$ of restricted Liouville numbers is a dense G_δ-set. The same is true for the intersection with $B_r := f_r((0,1))$. In view of the continuity of the f_r the pre-images $A_r := f_r^{-1}(L(\frac{a_r \bmod b_r}{c_r \bmod d_r}) \cap B_r)$ are also G_δ-sets; since each $f_r : (0,1) \to B_r$ is open and surjective, the pre-images A_r are dense in $(0,1)$ as well. Thus, the countable intersection

$$D = \left(L(\tfrac{a \bmod b}{c \bmod d}) \cap (0,1)\right) \cap \bigcap_r A_r$$

is again a dense G_δ-set (and in particular uncountable). It follows from

$$f_r(D) \subset f_r(A_r) \subset f_r(f_r^{-1}(L(\tfrac{a_r \bmod b_r}{c_r \bmod d_r}) \cap B_r)) \subset L(\tfrac{a_r \bmod b_r}{c_r \bmod d_r}) \cap B_r,$$

that $f_r(\xi) \in L(\frac{a_r \bmod b_r}{c_r \bmod d_r})$ for every $\xi \in D$. The theorem is proved.

5 Concluding Remarks

The problem of diophantine approximation with residue class constraints for the numerators and denominators of the rational approximations was first considered by Stanisław Hartman [37] and Jurjen Koksma [51]. More recently, Carsten Elsner [24, 25] investigated Liouville numbers having rational approximations with denominators from thin sets. However, his approach and aim is rather different from ours. Indeed, we could not find anything comparable to our results in the literature.

Of course, one could ask whether well-known results on Liouville numbers from the literature can be extended to restricted Liouville numbers. For example, Yann Bugeaud [12] proved that i) there exists a set of Liouville numbers which are not normal in any integer base and whose h-Hausdorff dimension is infinite for any sufficiently fast growing dimension function h, and ii) there exist Liouville numbers that are normal in all integer bases.

There are similar results on representations of real numbers as a sum of few summands or as a product of few factors. For instance, Marshall Hall [35] showed that every real number can be written as a sum of an integer and two regular continued fractions each of which having partial quotients less than or equal to four.[43]

Bagemihl and Władimir Seidel [3] used category theory for further studies in diophantine approximation theory; their result can be considered as a topological reformulation and extension of Kronecker's inhomogenous approximation theorem [52] for Hausdorff spaces. Also this question was raised by Erdős; moreover, there are several joint publications of Erdős with Bagemihl and Seidel on questions around topology in the 1950s, e.g., [4].

[43] Another much simpler example provides the middle third Cantor set $\mathcal{C}$. It is a folklore theorem that *every real number can be written as a sum of an integer and two elements of* $\mathcal{C}$.

Furthermore, let us remark that Goldbach's number $\xi = \sum 10^{-2^{n-1}}$ defined by (1.1) in the introduction is not a Liouville number. Nevertheless, it is a transcendental number as was first proved by Aubrey Kempner [49] in 1916; an alternative easy proof relies on Roth's theorem. It is remarkable that the sequence of partial quotients of the continued fraction expansion of ξ is bounded as was shown by Jeffrey Shallit [74]. By the way, a related transcendental quantity leads to the following trivial and completely useless criterion for Fermat primes: *there exist only finitely many Fermat primes* $f_n := 2^{2^n} + 1$ *if and only if*

$$\sum_{\substack{n\geq 0\\ f_n \text{ is prime}}} 10^{-f_n}$$

is rational. It is expected that there are no Fermat primes besides $f_0 = 3, f_1 = 5, f_2 = 17, f_3 = 257, f_4 = 65\,537$.

We conclude with a quotation from Wolfgang Schwarz's lecture notes [72] to a course on the history of number theory at Frankfurt University; in the preface Schwarz describes the concept of the course and the idea of historical studies[44]:

> Die Vorlesung ist damit ein Mittelding zwischen einer Geschichte der Zahlentheorie und einem zahlentheoretischen Ergebnisbericht. **Ein** Ziel geschichtlicher Untersuchungen, **Orientierung** zu vermitteln, könnte damit erreichbar sein.

In the course of writing this article the author has learned a lot from both, the mathematical and the historical point of view on Liouville numbers. It is not only the result that matters, but also the way we achieve it.

Acknowledgements It should be mentioned that the author wrote his doctorate under supervision of Prof. Georg Johann Rieger at Hanover University, and that he received his habilitation under guidance of Prof. Wolfgang Schwarz at Frankfurt University; he is very grateful to his academical teachers Prof. Rieger and Prof. Schwarz for their encouragement. Moreover, the author would like to thank Nicola Oswald for translating quotes from French to German and English, and to Prof. Carsten Elsner for informing about the state of the art of diophantine approximation with residue class conditions and correcting typos. Finally, the author is grateful to the organizers of the ELAZ Conference 2014 in Hildesheim for the great organization they did.

References

1. K. Alniaçik, É. Saias, Une remarque sur les G_δ-denses. Arch. Math. **62**, 425–426 (1994)
2. F. Bagemihl, A note on Scheeffer's theorem. Mich. Math. J. **2**, 149–150 (1953/1954)
3. F. Bagemihl, W. Seidel, A general principle involving Baire category, with applications to function theory and other fields. Proc. Natl. Acad. Sci. USA **39**, 1068–1075 (1953)

[44] Schwarz [72, p. 1]; English translation: "The course is thus a medium between a history of number theory and a report on number-theoretical results. **One** aim of historical investigations to give **orientation** could therefore be achieved." The boldfaced words are as in the original.

4. F. Bagemihl, P. Erdős, W. Seidel, Sur quelques propriétés frontières des fonctions holomorphes définies par certains produits dans le cercle-unité. Ann. Sci. Éc. Norm. Super. **70**, 135–147 (1953)
5. R.L. Baire, Sur les fonctions de variables réelles. Ann. di Mat. Pura ed applicata **3**, 1–123 (1899)
6. S. Banach, Über die Baire'sche Kategorie gewisser Funktionenmengen. Stud. Math. **3**, 174–179 (1931)
7. J. Barone, A. Novikoff, The Borel law of normal numbers, the Borel zero-one law, and the work of van Vleck. Hist. Math. **4**, 43–65 (1977)
8. J. Barone, A. Novikoff, A history of the axiomatic formulation of probability from Borel to Kolmogorov: Part I. Arch. Hist. Exact Sci. **18**, 123–190 (1978)
9. C.E. Blair, The Baire category theorem implies the principle of dependent choices. Bull. Acad. Polon. Sci. **25**, 933–934 (1977)
10. É. Borel, Les probabilités dénombrables et leurs applications arithmétiques. Rend. Circ. Matematico di Palermo **27**, 247–271 (1909)
11. W. Brito, *El Teorema de Categoría de Baire y aplicaciones* (Universidad de los Andes, Venezuela, 2011)
12. Y. Bugeaud, Nombres de Liouville et nombres normaux. C. R. Math. Acad. Sci. Paris **335**, 117–120 (2002)
13. E.B. Burger, On Liouville decompositions in local fields. Proc. Am. Math. Soc. **124**, 3305–3310 (1996)
14. E.B. Burger, R. Tubbs, *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory* (Springer, New York, 2004)
15. G. Cantor, Ueber eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen. J. Reine Angew. Math. **LXXVII**, 258–263 (1873)
16. G. Cantor, Über unendliche, lineare Punktmannigfaltigkeiten V. Math. Ann. **21**, 545–591 (1883)
17. G. Cantor, Ludwig Scheffer (1859–1885). Necrolog. Bibl. Math. 197–199 (1885)
18. G. Cantor, Ueber eine elementare Frage der Mannigfaltigkeitslehre. Jahresbericht der Deutschen Mathematiker-Vereinigung **1**, 75–78 (1892)
19. J. Cavaillès, E. Noether, *Briefwechsel Cantor-Dedekind*. Actualités Scientifiques et Industrielles, vol. 518 (Hermann, Paris, 1937)
20. J.W. Dauben, The trigonometric background to Georg Cantor's theory of sets. Arch. Hist. Exact Sci. **7**, 181–216 (1971)
21. O. Deiser, *Relle Zahlen* (Springer, Berlin, 2007)
22. P. du Bois-Reymond, Der Beweis des Fundamentalsatzes der Integralrechnung. Math. Ann. **16**, 115–128 (1880)
23. P. Dugac, Notes et documents sur la vie et l'oeuvre de René Baire. Arch. Hist. Exact Sci. **15**, 297–383 (1975/1976)
24. C. Elsner, On rational approximations with denominators from thin sets. Abh. Math. Sem. Univ. Hamburg **69**, 229–235 (1999)
25. C. Elsner, On rational approximations with denominators from thin sets. II. Abh. Math. Sem. Univ. Hamburg **72**, 35–45 (2002)
26. P. Erdős, Some remarks on set theory. Ann. Math. **44**, 643–646 (1943)
27. P. Erdős, Representations of real numbers as sums and products of Liouville numbers. Mich. Math. J. **9**, 59–60 (1962)
28. P. Erdős, Some personal and mathematical reminiscences of Kurt Mahler. Aust. Math. Soc. Gaz. **16**, 1–2 (1989)
29. L. Euler, Introduction to analysis of the infinite. Book I, translated by J.D. Blanton (Springer, New York, 1988)
30. G. Faber, Über stetige Funktionen. (Zweite Abhandlung). Math. Ann. **69**, 372–443 (1910)
31. H. Gispert, La théorie des ensembles en France avant la crise de 1905: Baire, Borel, Lebesgue . . . et tous les autres. Rev. Hist. Math. **1**, 39–81 (1995)

32. D. Gravé, Sur les lignes composées de parties rectilignes. C. R. Acad. Sci. Paris **127**, 1005–1007 (1898)
33. R. Gray, Georg Cantor and transcendental numbers. Am. Math. Mont. **101**, 819–832 (1994)
34. J. Gray, *Plato's Ghost* (Princeton University Press, Princeton, 2008)
35. M. Hall Jr., On the sum and product of continued fractions. Ann. Math. **28**, 966–993 (1947)
36. A. Harnack, *Die Elemente der Differential- und Integralrechnung. Zur Einführung in das Studium dargestellt* (Leipzig, Teubner, 1881)
37. S. Hartman, Sur une condition supplémentaire dans les approximations diophantiques. Colloq. Math. **2**, 48–51 (1949)
38. F. Hausdorff, *Grundzüge der Mengenlehre* (Veit & Co, Leipzig, 1914)
39. C. Hermite, Sur la fonction exponentielle. C. R. Acad. Sci. Paris **77**, 18–24, 74–79, 226–233, 285–293 (1873)
40. H. Herrlich, *Axiom of Choice* (Springer, Berlin, 2006)
41. I.N. Herstein, I. Kaplansky, *Matters Mathematical* (Harper & Row, New York, 1974); reprinted by Chelsea 1978
42. D. Hilbert, Über das Unendliche. Math. Ann. **95**, 161–190 (1926)
43. M. Hindry, J.H. Silverman, *Diophantine Geometry* (Springer, Berlin, 2000)
44. A. Hurwitz, Ueber die Entwickelung der allgemeinen Theorie der analytischen Functionen in neuerer Zeit. Verh. Intern. Math. Congr. **1**, 91–112 (1897)
45. H.J. Ilgauds, W. Purkert, *Georg Cantor* (Birkhäuser, Basel, 1987)
46. K.-H. Indlekofer, L.G. Lucht, J. Steuding, Obituary for Wolfgang Schwarz. Jahresber. Dtsch. Math.-Ver. **116**, 153–169 (2014)
47. S.H. Jones, Applications of the Baire category theorem. Real Anal. Exch. **23**, 363–394 (1997/1998)
48. A. Kanamori, Set theory from Cantor to Cohen, in *Sets and Extensions in the Twentieth Century*, ed. by D.M. Gabbay et al. Handbook of the History of Logic, vol. 6 (Elsevier, Boston, 2012), pp. 1–71
49. A.J. Kempner, On transcendental numbers. Am. M.S. Bull. **22**, 284–285 (1916)
50. E. Knobloch, Beyond Cartesian limits: Leibniz's passage from algebraic to 'transcendental' mathematics. Hist. Math. **33**, 113–131 (2006)
51. J.F. Koksma, Sur l'approximation des nombres irrationnels sous une condition supplementaire. Simon Stevin **28**, 199–202 (1951)
52. L. Kronecker, Die Periodensysteme von Funktionen reeller Variablen. Ber. d. K. Preuß. Ak. d. Wiss. Berl. 1071–1080 (1884)
53. D. Laugwitz, Debates about infinity in mathematics around 1890: the Cantor-Veronese controversy, its origins and its outcome. NTM (N.S.) **10**, 102–126 (2002)
54. J. Liouville, Remarques relatives 1° à des classes très-étendues de quantités dont la valeur n'est ni rationelle ni même réductible à des irrationnelles algébriques; 2° à un passage du livre des Principes où Newton calcule l'action exercée par une sphére sur un point extérieur. C.R. Acad. Sci. Paris **18**, 883–885 (1844)
55. J. Liouville, Nouvelle démonstration d'un théorème sur les irrationnelles algébriques. C.R. Acad. Sci. Paris **18**, 910–911 (1844)
56. J. Liouville, Sur des classes très-étendus de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébrique. Liouville J. **16**, 133–142 (1851)
57. J. Lützen, *Joseph Liouville, 1809–1882: Master of Pure and Applied Mathematics* (Springer, Berlin, 1990)
58. G.R. Mac Lane, On a conjecture by Erdős, Herzog, and Piranian. Mich. Math. J. **2**, 147–148 (1953)
59. E. Maor, *To Infinity and Beyond* (Princeton University Press, Princeton, 1987)
60. S. Mazurkiewicz, Sur les fonctions non derivables. Stud. Math. **3**, 92–94 (1931)
61. Z.A. Melzak, On the algebraic closure of a plane set. Mich. Math. J. **9**, 61–64 (1962)
62. G.H. Moore, *Zermelo's Axiom of Choice: Its Origins, Development, and Influence* (Springer, New York, 1982)

63. L. Olsen, Applications of multifractal divergence points to sets of numbers defined by their N-adic expansion. Math. Proc. Camb. Philos. Soc. **136**, 139–165 (2004)
64. W.F. Osgood, Ueber die ungleichmässige Convergenz und die gliedweise Integration der Reihen. Gött. Nachr. 288–291 (1896)
65. W.F. Osgood, Non-uniform convergence and the integration of series term by term. Am. J. Math. **19**, 155–190 (1897)
66. W.F. Osgood, On the existence of the Green's function for the most general simply connected plane region. Trans. A.M.S. **1**, 310–314 (1900)
67. J.C. Oxtoby, *Measure and Category* (Springer, New York, 1971)
68. G.J. Rieger, Über die Lösbarkeit von Gleichungssystemen durch Liouville-Zahlen. Arch. Math. **26**, 40–43 (1975)
69. L. Scheeffer, Zur Theorie der stetigen Funktionen einer reellen Veränderlichen. Acta Math. **5**, 183–194, 279–296 (1884)
70. T. Schneider, *Einführung in die Transzendenten Zahlen*, 2nd edn. (Springer, New York, 1957)
71. W. Schwarz, Liouville-Zahlen und der Satz von Baire. Math.-Phys. Semesterber. **24**, 84–87 (1977)
72. W. Schwarz, *Aus der Geschichte der Zahlentheorie*. Lecture Notes of a Course Held at Frankfurt University 2000/2001 with Supplements (2000/2001). Available at www.math.uni-frankfurt.de/~schwarz/schwarz/g_ztws98.pdf
73. K. Senthil Kumar, R. Thangadurai, M. Waldschmidt, Liouville numbers and Schanuel's Conjecture. Arch. Math. **102**, 59–70 (2014)
74. J. Shallit, Simple continued fractions for some irrational numbers. J. Number Theor. **11**, 209–217 (1979)
75. W. Sierpiński, Sur la dualité entre la première categorie et la mesure nulle. Fund. Math. **22**, 276–280 (1934)
76. W. Sierpiński, *General Topology* (University of Toronto Press, Toronto, 1952)
77. H.J.S. Smith, On the integration of discontinuous functions. Proc. Lond. Math. Soc. **6**, 140–153 (1874)
78. H. Steinhaus, Anwendungen der Funktionalanalysis auf einige Fragen der reellen Funktionentheorie. Stud. Math. **1**, 51–81 (1929)
79. E.B. van Vleck, A proof of some theorems on pointwise discontinuous functions. Trans. A.M.S. **8**, 189–204 (1907)
80. E.B. van Vleck, On non-measurable sets of points, with an example. Trans. A.M.S. **9**, 237–244 (1908)
81. E.B. van Vleck, Current tendencies of mathematical research. Bull. A.M.S. **23**, 1–13 (1916)
82. K. Volkert, Die Geschichte der pathologischen Funktionen. Ein Beitrag zur Entstehung der mathematischen Methodologie. Arch. Hist. Exact Sci. **37**, 193–232 (1987)
83. V. Volterra, Alcune osservazioni sulle funzioni punteggiate discontinue. Giornale di Matematiche **19**, 76–86 (1881)
84. H. Weber, Leopold Kronecker. Math. Ann. **43**, 1–25 (1893)
85. E. Zermelo, Beweis, daß jede Menge wohlgeordnet werden kann. Math. Ann. **59**, 514–516 (1904)

Natural Boundaries of Power Series with Multiplicative Coefficients in Algebraic Number Fields

Friedemann Tuttas

Dedicated to the memory of Wolfgang Schwarz

Abstract For an algebraic number field $K \neq \mathbb{Q}$ we prove that the unit disc is a natural boundary of the power series $\sum_{\mathfrak{a}\neq\mathfrak{o}} z^{N(\mathfrak{a})}$, $\mathfrak{a}$ running through the integral ideals of K and N denoting the norm function. As an application, we deduce the same result for power series $\sum_{\mathfrak{a}\neq\mathfrak{o}} g(\mathfrak{a})\, z^{N(\mathfrak{a})}$ with specific multiplicative coefficients $g(\mathfrak{a})$ thereby extending known results to algebraic number fields.

Keywords Algebraic number fields • Analytic continuation • Multiplicative arithmetic functions • Power series

2010 Mathematics subject classification: Primary 11N37; Secondary 30B40

1 Introduction

Functions $f\colon \mathbb{N} \to \mathbb{C}$ satisfying $f(1) = 1$ and $f(mn) = f(m)f(n)$ for $(m, n) = 1$ are called multiplicative. Under certain general conditions on f the generating power series

$$P(f, z) = \sum_{n=1}^{\infty} f(n)\, z^n \tag{1.1}$$

converges and represents an analytic function on the open unit disk $\mathbb{U} := \{z \in \mathbb{C} : |z| < 1\}$. The classical problem of analytic continuation of $P(f, z)$ beyond $\partial\mathbb{U}$ was studied in [5, 6]. In particular, for a large class $\mathscr{K}$ of multiplicative functions f, Lucht [5, Theorem 4] provides an equivalent arithmetical characterization of the

F. Tuttas (✉)
Hasengartenstrasse 13 B, 65189 Wiesbaden, Germany
e-mail: friedemann.tuttas@o2online.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_30

singular behavior of $P(f,z)$ on $\partial\mathbb{U}$. This can be applied to many important arithmetic functions, especially to functions $f \in \mathscr{W}_0$ characterized by Wirsing [7, Satz 1] (for the definition of $\mathscr{W}_0$ see [5, p. 368]).

The aim of this paper is to transfer the above-mentioned results to complex valued multiplicative functions defined on the set $I_0(K)$ of non-zero integral ideals of an algebraic number field K. Functions $g: I_0(K) \to \mathbb{C}$ satisfying $g(\mathfrak{e}) = 1$ for $\mathfrak{e} = (1)$ and $g(\mathfrak{ab}) = g(\mathfrak{a})\,g(\mathfrak{b})$ for $(\mathfrak{a},\mathfrak{b}) = \mathfrak{e}$ are called multiplicative. The identity function $n \mapsto I(n) = n$ for $n \in \mathbb{N}$ then corresponds to the norm function $\mathfrak{a} \mapsto N_K(\mathfrak{a})$ counting the residue classes modulo $\mathfrak{a}$. In particular, for $K = \mathbb{Q}$ we have $N_{\mathbb{Q}}(\mathfrak{n}) = n$ if $\mathfrak{n} = (n)$. For any algebraic number field K, N_K is completely multiplicative, i.e. $N_K(\mathfrak{ab}) = N_K(\mathfrak{a})\,N_K(\mathfrak{b})$ for all $\mathfrak{a},\mathfrak{b} \in I_0(K)$, and the power series (1.1) takes the form

$$P(K,g,z) = \sum_{\mathfrak{a}\in I_0(K)} g(\mathfrak{a})\, z^{N(\mathfrak{a})} \qquad (N(\mathfrak{a}) = N_K(\mathfrak{a})). \tag{1.2}$$

The usual multiplicative functions on $\mathbb{N}$ are related to those on $I_0(K)$, as (1.2) may be rewritten as

$$P(K,g,z) = \sum_{n=1}^{\infty} G(n)\, z^n$$

with

$$G(n) = \sum_{N(\mathfrak{a})=n} g(\mathfrak{a}), \tag{1.3}$$

and G is multiplicative if g is multiplicative (compare [3, § 41]). Provided that $G \in \mathscr{W}_0$, [5] entails an immediate characterization of the singular behavior of $P(K,g,z)$ for $z \in \partial\mathbb{U}$.

Observe that the constant function $1: I_0(K) \to \{1\}$ with $1(\mathfrak{a}) = 1$ for all $\mathfrak{a} \in I_0(K)$ corresponds to the function F with

$$F(n) = \sum_{N(\mathfrak{a})=n} 1, \tag{1.4}$$

the number of integral ideals of K with norm n. In Sect. 2 we shall see that F does not necessarily belong to $\mathscr{W}_0$ (Remark 2.7). Hence the results of [5] cannot be applied to F, in general.

In Sect. 2, we therefore introduce certain classes $\mathscr{K}_e$ for $e \in \mathbb{N}$ such that $\mathscr{K} \subseteq \bigcup \mathscr{K}_e$ and corresponding classes $\mathscr{W}_e$ refining $\mathscr{W}_0$ accordingly. As the methods and results of [5] then can be easily transferred from $\mathscr{K}$ and $\mathscr{W}_0$ to $\mathscr{K}_e$ and $\mathscr{W}_e$, we obtain equivalent characterizations of the singular behavior of $P(K,g,z)$ for $z \in \partial\mathbb{U}$ in case of $G \in \mathscr{K}_e$ and $G \in \mathscr{W}_e$ (Theorems 2.3 and 2.6).

For the application of Theorems 2.3 and 2.6 to specific functions $g: I_0(K) \to \mathbb{C}$ it remains to verify that $G \in \mathscr{W}_e$ for some $e \in \mathbb{N}$. Actually this is not even evident for the simple constant function 1 corresponding to F via (1.4). For the rational number field $K = \mathbb{Q}$ we have $P(\mathbb{Q}, 1, z) = \frac{z}{1-z}$ for $z \in \mathbb{U}$, which obviously has an analytic continuation beyond $\partial\mathbb{U}$. But this does no longer hold for $K \neq \mathbb{Q}$. In Sect. 3 we prove the main result of this paper: If $K \neq \mathbb{Q}$, then $F \in \mathscr{W}_e$ for some $e \in \mathbb{N}$, and

$$\sum_{\mathfrak{a} \in I_0(K)} z^{N(\mathfrak{a})}$$

has no analytic continuation beyond $\partial\mathbb{U}$ (Theorem 3.1). The proof uses results of algebraic number theory and can also be used to characterize those F with $F \in \mathscr{W}_0$ (Remark 3.2).

Finally, in Sect. 4 we discuss further specific arithmetic functions $g: I_0(K) \to \mathbb{C}$ to find that known negative results concerning the analytic continuation of $P(\mathbb{Q}, f, z)$ beyond $\partial\mathbb{U}$ remain valid when considered in algebraic number fields $K \neq \mathbb{Q}$. The examples permanently use Theorem 3.1.

2 The Classes $\mathscr{K}_e$ and $\mathscr{W}_e$

We begin with defining the classes $\mathscr{K}_e^*$ and $\mathscr{K}_e$ of multiplicative functions $f: \mathbb{N} \to \mathbb{C}$ for $e \in \mathbb{N}$ which represent a slight modification of the classes $\mathscr{K}^*$ and $\mathscr{K}$ in [5]. Let $M(f, x)$ denote the sum

$$M(f, x) = \sum_{n \le x} f(n).$$

Definition 2.1 *For $e \in \mathbb{N}$ let $\mathscr{K}_e^*$ consist of all multiplicative functions $f: \mathbb{N} \to \mathbb{C}$ with the following properties:*

(a) *There exists some $s \in \mathbb{C}$ with $\sigma = \operatorname{Re} s \ge 0$ and a slowly oscillating function L such that for each $q \in \mathbb{N}$, $(q, e) = 1$, there is a constant $c_q \in \mathbb{C}$ with*

$$M(f\chi, x) = \begin{cases} c_q\, x^s\, L(x) + \mathrm{o}\left(x^\sigma\, |L(x)|\right) & \text{if } \chi = \chi_0 \bmod q \\ \mathrm{o}\left(x^\sigma\, |L(x)|\right) & \text{if } \chi \neq \chi_0 \bmod q \end{cases} \qquad (x \to \infty)$$

for all characters $\chi \bmod q$.

(b) *There is some $q^* \in \mathbb{N}$ with $(q^*, e) = 1$ and $c_{q^*} \neq 0$.*

(c) *For each prime p there is some $\varepsilon > 0$ such that the series*

$$\sum_{\nu=2}^{\infty} \frac{|f(p^\nu)|}{p^{(\sigma-\varepsilon)\nu}}$$

converges.

Here $L\colon [0,\infty) \to \mathbb{C}$ is called slowly oscillating if L is measurable and $L(x) \sim L(cx)$ for $x \to \infty$, uniformly for $1 \le c \le 2$.

In contrast to $\mathscr{K}^*$, the definition of $\mathscr{K}_e^*$ requires coprimality of q, e and of q^*, e in (a) and (b). Clearly $\mathscr{K}_1^* = \mathscr{K}^*$. Both $f \in \mathscr{K}^*$ and $c_a \neq 0$ for some $a \in \mathbb{N}$ entail that $f \in \mathscr{K}_e^*$ for all $e \in \mathbb{N}$ with $(e,a) = 1$. Hence $\mathscr{K}^* \subseteq \bigcup_{e \ge a} \mathscr{K}_e^*$ for all $a \in \mathbb{N}$.

To formulate Lemma 3, Corollary 2 and Theorem 2 in [5] for $f \in \mathscr{K}_e^*$ only require a redactional revision which does not change the assertions and may be left to the reader. We note that the number s from Definition 2.1 is uniquely determined: $s = s_f$.

Definition 2.2 *For $e \in \mathbb{N}$ let $\mathscr{K}_e$ be the class of functions $f \in \mathscr{K}_e^*$ satisfying the additional property:*

(d) $\lim_{x\to\infty} x^s L(x)$ *does not exist.*

Similarly we see that $\mathscr{K}_1 = \mathscr{K}$ and $\mathscr{K} \subseteq \bigcup_{e \ge a} \mathscr{K}_e$ for all $a \in \mathbb{N}$.

For the function classes under consideration the power series $P(f,z)$ converges for all $z \in \mathbb{U}$, and the characterization of functions $f \in \mathscr{K}$ having $\partial\mathbb{U}$ as natural boundary according to [5, Theorem 4] transfers to functions $f \in \mathscr{K}_e$:

Theorem 2.3 *Let $f \in \mathscr{K}_e$, $s = s_f$. Then the following assertions are equivalent:*

(A) *$P(f,z)$ has $\mathbb{U}$ as natural boundary.*
(B) *There are infinitely many prime powers p^β with $p \nmid e$ such that*

$$\eta_\beta(f,p,s) \neq \frac{1}{\varphi(p)} \frac{f(p^{\beta-1})}{p^{(\beta-1)s}},$$

where $\eta_\beta(f,p,s) = \sum_{\nu=\beta}^{\infty} \frac{f(p^\nu)}{p^{\nu s}}$ for $\beta \in \mathbb{N}$.

Next we recall the class of multiplicative functions investigated by Wirsing [7].

Definition 2.4 *Let $\mathscr{W}$ denote the set of multiplicative functions $f\colon \mathbb{N} \to \mathbb{C}$ with the following properties:*

(a) $f(n) \ge 0$ *for $n \in \mathbb{N}$.*
(b) $\sum_{p,\nu\ge 2} \frac{f(p^\nu)}{p^{(1-\varepsilon)\nu}} < \infty$ *for some $\varepsilon > 0$.*
(c) $\lim_{x\to\infty} \frac{1}{x} \sum_{p\le x} f(p) \log p \neq 0$ *exists.*

For $e \in \mathbb{N}$ let further $\mathscr{W}_e$ be the class of functions $f \in \mathscr{W}$ such that for each $q \in \mathbb{N}$ with $(q,e) = 1$ and each character $\chi \bmod q$, $\chi \neq \chi_0$, the following holds in addition:

(d) $\lim_{x\to\infty} \frac{1}{x} \sum_{p\le x} f(p)\,\chi(p)\,\log p$ *exists,*
(e) $\sum_p \frac{f(p)(1-\operatorname{Re}\chi(p))}{p}$ *diverges.*

Note that condition (b) in Definition 2.4 is a slight generalization of local restrictions imposed on the values of f at the prime powers p^ν with $\nu \geq 2$ in Wirsing's paper [7] such that, in particular, Satz 1 and Satz 2 in [7] remain true. This yields that $\mathscr{W}_e \subseteq \mathscr{K}_e$. We summarize:

Corollary 2.5 *$\mathscr{W}_e \subseteq \mathscr{K}_e$ for all $e \in \mathbb{N}$, $s_f = 1$ for any $f \in \mathscr{W}_e$, and $\mathscr{W}_0 = \mathscr{W}_1$.*

As an immediate consequence we obtain the following result for multiplicative functions $g: I_0(K) \to \mathbb{C}$.

Theorem 2.6 *Let K be an algebraic number field, $g: I_0(K) \to \mathbb{C}$ a multiplicative function and G defined by (1.3). If there is some $e \in \mathbb{N}$ such that $G \in \mathscr{W}_e$, then the following assertions are equivalent:*

(A) *$P(K, g, z)$ has $\mathbb{U}$ as natural boundary.*
(B) *There are infinitely many prime powers p^β ($\beta \in \mathbb{N}$) with $p \nmid e$ and*

$$\eta_\beta(G, p, 1) \neq \frac{1}{\varphi(p)} \frac{G(p^{\beta-1})}{p^{\beta-1}}.$$

In the introduction we noted that, in general, $F \in \mathscr{W}_0$ is not true which is justified here:

Remark 2.7 There are algebraic number fields $K \neq \mathbb{Q}$ such that the function $F: \mathbb{N} \to \mathbb{Z}$ associated with the constant function $1: I_0(K) \to \{1\}$ according to (1.4) does not belong to $\mathscr{W}_0$.

For, if K is an algebraic number field containing the mth cyclotomic field $\mathbb{Q}\left(e^{\frac{2\pi i}{m}}\right)$ then, according to [1, Lemma 3, p. 351], $N(\mathfrak{p}) \equiv 1 \bmod m$ holds for every prime ideal $\mathfrak{p}$ which does not divide m. For $m \geq 3$ there exists a non-principal character $\chi \bmod m$. Hence

$$\sum_{\substack{p \leq x \\ p \nmid m}} \frac{F(p)(1 - \operatorname{Re} \chi(p))}{p} = \sum_{\substack{p = N(\mathfrak{p}) \leq x \\ p \nmid m}} \frac{1 - \operatorname{Re} \chi(p)}{p} = 0,$$

which contradicts Definition 2.4 (e).

3 The Power Series $\sum_{\mathfrak{a} \in I_0(K)} z^{N(\mathfrak{a})}$

In the sequel we study the special case $g = 1$.

Theorem 3.1 *For every algebraic number field $K \neq \mathbb{Q}$ the power series*

$$P(K, 1, z) = \sum_{\mathfrak{a} \in I_0(K)} z^{N(\mathfrak{a})}$$

converges in $\mathbb{U}$ and has $\partial\mathbb{U}$ as natural boundary.

Proof We have to verify that the function F associated with 1 according to (1.4) satisfies

(I) $F \in \mathscr{W}$,
(II) $F \in \mathscr{W}_e$ for some $e \in \mathbb{N}$,
(III) F satisfies condition (B) from Theorems 2.3 and 2.6.

Proof of (I): Condition (a) of Definition 2.4 is satisfied as is (c) by Landau's prime ideal theorem, for

$$\sum_{p \le x} F(p) \sim \frac{x}{\log x} \qquad (x \to \infty),$$

and partial summation implies (c).
To verify (b) we estimate $F(p^\nu)$. Let $[K : \mathbb{Q}] = n$ and let $\mathfrak{a}$ an integral ideal of K with $N(\mathfrak{a}) = p^\nu$. Then the prime ideal divisors $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of $\mathfrak{a}$ satisfy

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}, \quad \alpha_j \in \mathbb{N}, \quad N(\mathfrak{p}_\varrho) = p^{\nu_\varrho} \text{ with } \nu_\varrho \in \mathbb{N}, \quad r \le n.$$

Taking the norm on both sides yields $p^\nu = p^{\nu_1 \alpha_1} \cdots p^{\nu_r \alpha_r}$ or, equivalently,

$$\nu_1 \alpha_1 + \cdots + \nu_r \alpha_r = \nu \qquad (\alpha_\varrho, \nu_\varrho \in \mathbb{N},\ r \le n).$$

For the number $L(\nu)$ of solutions of this equation we obtain with the divisor function τ,

$$L(\nu) = \sum_{\substack{\nu_1, \dots, \nu_r \ge 1 \\ \nu_1 \alpha_1 + \cdots + \nu_r \alpha_r = \nu \\ r \le n}} 1 \le \sum_{\substack{m_1, \dots, m_r \ge 1 \\ m_1 + \cdots + m_r = \nu \\ r \le n}} \tau(m_1) \cdots \tau(m_r)$$

$$\le \sum_{r=1}^{n} \nu^r \sum_{\substack{m_1, \dots, m_r \ge 1 \\ m_1 + \cdots + m_r = \nu}} 1 \le \sum_{r=1}^{n} \nu^r \cdot \nu^r \le (\nu + 1)^{2n}.$$

This entails $F(p^\nu) \le L(\nu) \le (\nu + 1)^{2n}$, and (b) is satisfied for $0 < \varepsilon < \frac{1}{2}$.
Proof of (II): For $q \in \mathbb{N}$ let $L = K(\zeta)$ with $\zeta = e^{\frac{2\pi i}{q}}$ the cyclotomic field over K. Then L is a normal extension of K with an abelian Galois group, isomorphic to some subgroup of the prime residue group modulo q. The Kronecker–Weber theorem implies the existence of some $m \in \mathbb{N}$ such that $[L : K] = \varphi(q)$ for all q, $(q, m) = 1$; see Hasse [2, Satz 133, p. 196]. For those q the Galois group of L/K is isomorphic to the prime residue class group mod$q$ and, in particular, abelian.
To verify properties (d) and (e) of Definition 2.4 we use Chebotarev's density theorem. We recall the following:
Let $\mathfrak{p}$ be a prime ideal of K and $\mathfrak{P}$ a prime ideal divisor of $\mathfrak{p}$ in L. Then for unramified $\mathfrak{p}$ the Frobenius automorphism σ uniquely determined by $\mathfrak{p}$ and $\mathfrak{P}$

satisfies

$$\xi^{N(\mathfrak{p})} \equiv \sigma(\xi) \bmod \mathfrak{P}$$

for all integral $\xi \in L$. This holds for any normal field extension L of K. If $\tau \in G = \mathrm{Gal}\,(L/K)$, then the conjugate prime ideal $\tau(\mathfrak{P})$ of $\mathfrak{P}$ corresponds to the Frobenius automorphism $\tau\sigma\tau^{-1}$. The conjugacy class of σ in G is independent of the prime divisors of $\mathfrak{p}$ in L and is denoted by the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ $\left(= \{\tau\sigma\tau^{-1} : \tau \in G\}\right)$. For a conjugacy class C of G let further

$$\pi_C(x, L/K) = \sum_{\substack{\mathfrak{p} \text{ unramified in } L \\ N(\mathfrak{p}) \le x \\ \left(\frac{L/K}{\mathfrak{p}}\right) = C}} 1.$$

Chebotarev's density theorem says: *Let K be an algebraic number field and L a finite normal field extension of K with Galois group G. Then*

$$\pi_C(x, L/K) \sim \frac{|C|}{|G|} \frac{x}{\log x} \qquad (x \to \infty).$$

This asymptotic equation suffices for our purposes, for a version with remainder term see Lagarias and Odlyzko [4].

We apply this theorem to $L = K(\zeta)$ with $\zeta = e^{\frac{2\pi i}{q}}$ and $(q, m) = 1$ where m was chosen such that $|G| = \varphi(q)$ for $(q, m) = 1$. Letting $e = m$ we have to verify conditions (d) and (e) of Definition 2.4.

As G is abelian the conjugacy classes of G are singletons. Denote the automorphism $\zeta \mapsto \zeta^a$ by σ_a. Then $G = \{\sigma_a : (a, q) = 1\}$. Let $\mathfrak{p}$ neither divide the relative discriminant of L/K nor the discriminant d of the polynomial $x^q - 1$, and let $\left(\frac{L/K}{\mathfrak{p}}\right) = \{\sigma_a\}$ for some a, $(a, q) = 1$. Then, for all integral $\xi \in L$ and all prime divisors $\mathfrak{P}$ of $\mathfrak{p}$,

$$\xi^{N(\mathfrak{p})} \equiv \sigma_a(\xi) \bmod \mathfrak{P},$$

hence

$$\xi^{N(\mathfrak{p})} \equiv \sigma_a(\xi) \bmod \mathfrak{p},$$

and thus

$$\zeta^{N(\mathfrak{p})} \equiv \zeta^a \bmod \mathfrak{p}.$$

Suppose that $\zeta^{N(\mathfrak{p})} \neq \zeta^a$, then $\zeta^{N(\mathfrak{p})} - \zeta^a$ divides the discriminant d so that $\mathfrak{p} \mid d$, a contradiction. Therefore $\zeta^{N(\mathfrak{p})} = \zeta^a$, so $N(\mathfrak{p}) \equiv a \bmod q$. Now by Chebotarev's theorem

$$\sum_{\substack{N(\mathfrak{p}) \leq x \\ N(\mathfrak{p}) \equiv a \bmod q}} 1 \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \qquad (x \to \infty).$$

Since we can neglect prime ideals of higher degree this asymptotic relation yields

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} F(p) \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \qquad (x \to \infty).$$

Partial summation gives

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} F(p) \log p \sim \frac{1}{\varphi(q)} x \qquad (x \to \infty) \tag{3.1}$$

and

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{F(p)}{p} \sim \frac{1}{\varphi(q)} \log \log x \qquad (x \to \infty) \tag{3.2}$$

which implies (d),

$$\sum_{p \leq x} F(p)\, \chi(p) \log p = \sum_{a \bmod q}^{*} \chi(a) \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} F(p) \log p = \mathrm{o}(x) \qquad (x \to \infty)$$

for each character $\chi \neq \chi_0 \bmod q$, $(q, m) = 1$. Here $*$ indicates summation over the prime residue classes $\bmod q$.
In the same way we obtain (e), namely, for $\chi \neq \chi_0 \bmod q$, $(q, m) = 1$, by (3.2)

$$\begin{aligned} \sum_{p \leq x} \frac{F(p)\big(1 - \operatorname{Re} \chi(p)\big)}{p} &= \sum_{a \bmod q}^{*} \big(1 - \operatorname{Re} \chi(a)\big) \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{F(p)}{p} \\ &= \frac{1 + \mathrm{o}(1)}{\varphi(q)} \log \log x \cdot \sum_{a \bmod q}^{*} \big(1 - \operatorname{Re} \chi(a)\big) \qquad (x \to \infty). \end{aligned} \tag{3.3}$$

For $q \geq 3$ and $\chi \neq \chi_0 \bmod q$ there is some $a \in \mathbb{N}$ with $(a, q) = 1$ and $\chi(a) \neq 1$. Hence $1 - \operatorname{Re} \chi(a) > 0$, the sum factor in (3.3) does not vanish, and the series (e) diverges.

Proof of (III): We have $s_F = 1$. As in the proof of (II), let $m \in \mathbb{N}$ be such that $F \in \mathscr{W}_m$. Suppose that condition (B) of Theorem 2.6 is not valid for F. Then there are at most finitely many primes p with $F(p) = 0$, because otherwise (B) would hold for these p with $\beta = 2$.

For all sufficiently large primes $p > m$ exceeding the discriminant of K we have $F(p) \geq 1$, p is not divisible by any prime ideal square, and

$$\eta_1(F, p, 1) = \frac{1}{\varphi(p)}$$

for $\beta = 1$. It follows that $F(p^\nu) \geq 1$ for $\nu \geq 1$, and hence

$$\frac{1}{\varphi(p)} = \eta_1(F, p, 1) \geq \frac{1}{p} + \frac{1}{p^2} + \cdots = \frac{1}{\varphi(p)}\,.$$

Hence $F(p^\nu) = 1$ for $\nu \geq 1$, and the ideals (p) are prime ideals of first degree of K. Taking the norm yields $p^n = N\big((p)\big) = p$, so $n = [K : \mathbb{Q}] = 1$, that is $K = \mathbb{Q}$, which is a contradiction. Therefore F has to satisfy (B), which completes the proof of Theorem 3.1.

The proof of (III) could be simplified a little by observing the known fact that, for each $K \neq \mathbb{Q}$, $F(p) = 0$ holds for infinitely many primes p. Namely, let L be the normal closure of $K/\mathbb{Q}$, let $n = [K : \mathbb{Q}] \geq 2$, $N = [L : \mathbb{Q}]$, and let the functions attached to K and L, resp., according to (1.4) be denoted by F_K and F_L, resp. Then a prime p is totally split in L iff it is totally split in K, and we have for $x \to \infty$

$$\sum_{\substack{p \leq x \\ F_K(p) = n}} 1 = \sum_{\substack{p \leq x \\ F_L(p) = N}} 1 \sim \frac{1}{N} \frac{x}{\log x},$$

$$\sum_{p \leq x} F_K(p) = (1 + \mathrm{o}\,(1)) \frac{x}{\log x} \geq \sum_{\substack{p \leq x \\ 1 \leq F_K(p) \leq n}} 1 + \left(\frac{n-1}{N} + \mathrm{o}\,(1) \right) \frac{x}{\log x},$$

$$\sum_{\substack{p \leq x \\ F_K(p) = 0}} 1 = \sum_{p \leq x} 1 - \sum_{\substack{p \leq x \\ 1 \leq F_K(p) \leq n}} 1 \geq \left(\frac{n-1}{N} + \mathrm{o}\,(1) \right) \frac{x}{\log x}.$$

We mention that, for the same reason, a previous non-continuability criterion [6, Theorem 5] cannot be applied to F, as the requirement

$$\sum_{n \leq x} |F(n)|^2 = \mathrm{O}\,(x)$$

is not satisfied for $K \neq \mathbb{Q}$.

As regards the question when $F \in \mathscr{W}_0$, a partial answer was given in Remark 2.7. Using the argument in the proof of (II), we can now characterize the functions F belonging to $\mathscr{W}_0$.

Remark 3.2 For $K \neq \mathbb{Q}$ we have $F \in \mathscr{W}_0$ iff $\mathbb{Q}$ is the only (absolute) abelian subfield of K.

For, if K does not contain any abelian subfield $\neq \mathbb{Q}$, $K \cap \mathbb{Q}_m = \mathbb{Q}$ for all cyclotomic fields $\mathbb{Q}_m = \mathbb{Q}(\zeta)$, $\zeta = e^{\frac{2\pi i}{m}}$. According to Galois theory, we have for $L = K(\zeta)$

$$G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathbb{Q}_m/K \cap \mathbb{Q}_m) = \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}),$$

and thus $|G| = \varphi(m)$. Using the same argument as in the proof of (II), we obtain

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod m}} F(p) \sim \frac{1}{\varphi(m)} \frac{x}{\log x} \qquad (x \to \infty, (a, m) = 1),$$

and hence $F \in \mathscr{W}_0$. On the other side, if $K_0 = K \cap \mathbb{Q}_m \neq \mathbb{Q}$ for some $m \geq 3$, we have

$$G \cong \mathrm{Gal}(\mathbb{Q}_m/K_0) \cong H,$$

where H is a proper subgroup of the prime residue group modulo m. We can find a character $\chi \bmod m$, $\chi \neq \chi_0$, such that $\chi(a) = 1$ for all $a \in H$. According to the proof of (II), we have for each prime ideal $\mathfrak{p}$ of K (except at most finitely many) $N(\mathfrak{p}) \equiv a \bmod m$ for some $a \in H$. Therefore, for sufficiently large $p \geq p_0$, $F(p) = 0$ if $p \equiv b \bmod m$, $b \notin H$. It follows that $F(p)\big(1 - \mathrm{Re}\,\chi(p)\big) = 0$ for $p \geq p_0$, the series $\sum_p \frac{F(p)\left(1-\mathrm{Re}\,\chi(p)\right)}{p}$ is convergent and $F \notin \mathscr{W}_0$.

4 Examples

Let K be an algebraic number field, not necessarily distinct from $\mathbb{Q}$, and let $n = [K : \mathbb{Q}]$ be the degree of K over $\mathbb{Q}$. According to the proof of Theorem 3.1, fix $m \in \mathbb{N}$ such that $F \in \mathscr{W}_m$. In the sequel we consider specific multiplicative functions $g\colon I_0(K) \to \mathbb{C}$ so as to show that $\partial\mathbb{U}$ is the natural boundary of the corresponding power series $P(K, g, z)$. Again, with $G\colon \mathbb{N} \to \mathbb{C}$ given by (1.3),

$$G(n) = \sum_{N(\mathfrak{a})=n} g(\mathfrak{a}),$$

$G \in \mathscr{W}_m$ will follow from $F \in \mathscr{W}_m$. Then Theorem 2.6 applies and it remains to verify that condition (B) of this theorem holds.

All examples to be considered here show certain similarities which we outline first to clarify and shorten the argumentation.

First we will always have $G(n) \geq 0$ and $G(p) = F(p)\,c(p)$ with $c(p) = C + o(1)$ with some constant $C > 0$ for all primes $p \in \mathbb{P}$. It follows from Theorem 3.1 that conditions (a) and (c) of Definition 2.4 are satisfied. For the proof of convergence of the series in Definition 2.4 (b) for some $\varepsilon \in \left(0, \frac{1}{2}\right)$ we set

$$H(n) = \max\{g(\mathfrak{a}) : N(\mathfrak{a}) = n\}.$$

As g will only take non-negative real values in our examples, we see that $H(n) \geq 0$ and $0 \leq G(n) \leq F(n)\,H(n)$ for $n \in \mathbb{N}$. Therefore the convergence of the series in Definition 2.4 (b) is guaranteed by any inequality of the form

$$H(p^\nu) \leq \gamma(\nu + 1)^\alpha \tag{4.1}$$

with some constants $\alpha, \gamma \geq 0$ which might depend on n. Combined with the already proved inequality $F(p^\nu) \leq (\nu + 1)^{2n}$ this would imply $G(p^\nu) \leq \gamma(\nu + 1)^{2n+\alpha}$.

Conditions (d) and (e) of Definition 2.4 follow immediately from the above assumptions concerning $G(p)$ combined with (3.1) and (3.2). Altogether (4.1) yields $G \in \mathscr{W}_m$ and $s_G = 1$.

Suppose that condition (B) of Theorem 2.6 does not hold. Then for all sufficiently large primes $p \geq p_0 > m$ and all $a \in \mathbb{N}$,

$$\eta_a(G, p, 1) = \frac{1}{\varphi(p)} \frac{G(p^{a-1})}{p^{a-1}}.$$

Taking differences gives

$$\eta_a(G, p, 1) - \eta_{a+1}(G, p, 1) = \frac{G(p^a)}{p^a} = \frac{1}{\varphi(p)} \frac{1}{p^{a-1}} \left(G(p^{a-1}) - \frac{G(p^a)}{p}\right)$$

which entails that

$$G(p^a) = G(p^{a-1})$$

for all $a \in \mathbb{N}$ and $p \geq p_0$. Hence, for $a = 1$, $G(p) = F(p)\,c(p) = 1$. This is a contradiction since, according to the remark following the proof of Theorem 3.1, $F(p) = 0$ for infinitely many primes p.

As an intermediate result we note

Corollary 4.1 *Let $g: I_0(K) \to \mathbb{R}$ be a multiplicative function with non-negative values and $G: \mathbb{N} \to \mathbb{R}$ the multiplicative function associated with g according to (1.3). Suppose that $G(p) = F(p)\,c(p)$ where $c(p) = C + o(1)$ with some positive real constant C. If there are positive constants α, γ which may depend on n such that $H(p^\nu) \leq \gamma\,(\nu + 1)^\alpha$ for all prime powers p^ν with $\nu \in \mathbb{N}$, then $G \in \mathscr{W}_m$ and $\mathbb{U}$ is a natural boundary of $P(K, g, z)$.*

The first example deals with $\varphi(\mathfrak{a})$, the number of prime residue classes mod $\mathfrak{a}$.

Example 4.2 $\sum_{\mathfrak{a}\neq\mathfrak{o}} \varphi(\mathfrak{a})\, z^{N(\mathfrak{a})}$ has $\partial\mathbb{U}$ as natural boundary.

Proof It suffices to verify the assertion for $g(\mathfrak{a}) = \frac{\varphi(\mathfrak{a})}{N(\mathfrak{a})} = \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)$.

We have $G(p) = F(p)\left(1-\frac{1}{p}\right)$, hence $c(p) = 1-\frac{1}{p}$, $H(n) \leq 1$, and Corollary 4.1 implies the assertion.

For integral ideals $\mathfrak{a}$ of K and $k \in \mathbb{N}$ we may define the sum of divisors function by $\sigma_k(\mathfrak{a}) = \sum_{\mathfrak{d}|\mathfrak{a}} N^k(\mathfrak{d})$.

Example 4.3 $\sum_{\mathfrak{a}\neq\mathfrak{o}} \sigma_k(\mathfrak{a})\, z^{N(\mathfrak{a})}$ has $\partial\mathbb{U}$ as natural boundary.

Proof It suffices to verify the assertion for $g_k(\mathfrak{a}) = \frac{\sigma_k(\mathfrak{a})}{N^k(\mathfrak{a})}$.

We have $G_k(p) = F(p)\left(1+\frac{1}{p^k}\right)$, hence $c(p) = 1+\frac{1}{p^k}$. To show the convergence of the series in Definition 2.4 (b) we proceed as in the proof of Theorem 3.1, part (I), and set

$$\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} \text{ with } \alpha_\varrho \in \mathbb{N}, \quad N(\mathfrak{p}_\varrho) = p^{\nu_\varrho} \text{ with } \nu_\varrho \in \mathbb{N}, \quad r \leq n \tag{4.2}$$

for integral ideals $\mathfrak{a}$ of K with $N(\mathfrak{a}) = p^\nu$ and distinct prime ideals $\mathfrak{p}_\varrho$, $\varrho = 1, \ldots, r$. Then

$$g_k(\mathfrak{a}) = \frac{\sigma_k(\mathfrak{p}_1^{\alpha_1})}{N^k(\mathfrak{p}_1^{\alpha_1})} \cdots \frac{\sigma_k(\mathfrak{p}_r^{\alpha_r})}{N^k(\mathfrak{p}_r^{\alpha_r})} \leq \left(1 + \frac{\alpha_1}{p^{\nu_1 k}}\right) \cdots \left(1 + \frac{\alpha_r}{p^{\nu_r k}}\right) \leq (\nu+1)^n$$

and therefore $H(p^\nu) \leq (\nu+1)^n$. Corollary 4.1 establishes Example 4.3.

For integral ideals $\mathfrak{a}$ of K we define the divisor function by $\tau(\mathfrak{a}) = \sum_{\mathfrak{d}|\mathfrak{a}} 1$.

Example 4.4 $\sum_{\mathfrak{a}\neq\mathfrak{o}} \tau(\mathfrak{a})\, z^{N(\mathfrak{a})}$ has $\partial\mathbb{U}$ as natural boundary.

Proof We have $G(p) = 2F(p)$ and $c(p) = 2$. For the proof of convergence of the series in Definition 2.4 (b) we use (4.2) for integral ideals $\mathfrak{a}$ with $N(\mathfrak{a}) = p^\nu$ again to obtain

$$\nu_1\alpha_1 + \cdots + \nu_r\alpha_r = \nu,$$
$$(\alpha_1 + 1) + \cdots + (\alpha_r + 1) \leq \nu + r.$$

The arithmetic-geometric mean inequality yields

$$\tau(\mathfrak{a}) = (\alpha_1 + 1) \cdots (\alpha_r + 1) \leq \left(\frac{\nu + r}{r}\right)^r.$$

Therefore $H(p^\nu) \leq (\nu+1)^n$, and Corollary 4.1 implies the assertion.

With the Möbius function μ defined as usual for integral ideals of K, $\mu^2(\mathfrak{a})$ represents the characteristic function of the squarefree integral ideals $\mathfrak{a}$ of K.

Example 4.5 $\sum_{\mathfrak{a}\neq\mathfrak{o}} \mu^2(\mathfrak{a})\, z^{N(\mathfrak{a})}$ has $\partial\mathbb{U}$ as natural boundary.

Proof Corollary 4.1 can be applied since we have $G(p) = F(p)$, $c(p) = 1$, $H(n) \leq 1$.

References

1. S.I. Borewicz, I.R. Šafarevič, *Zahlentheorie* (Birkhäuser Verlag, Basel, 1966)
2. H. Hasse, *Vorlesungen über Klassenkörpertheorie* (Physica-Verlag, Würzburg, 1967)
3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Nachdruck Chelsea, New York, 1970)
4. J.C. Lagarias, A.M. Odlyzko, Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields (L-Functions and Galois Properties)*, ed. by A. Fröhlich (Academic Press, New York, 1977), pp. 409–464
5. L. Lucht, Power series with multiplicative coefficients. Math. Z. **177**, 359–374 (1981)
6. L. Lucht, F. Tuttas, Mean values of multiplicative functions and natural boundaries of power series with multiplicative coefficients. J. Lond. Math. Soc. **19**(2), 25–34 (1979)
7. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. Math. Ann. **143**, 75–102 (1961)

A Minimal Proof of a Result of Hardy

Eduard Wirsing

To the memory of my friend Wolfgang

Abstract A simple proof of Hardy's theorem on the existence of power series which converge uniformly on the unit circle but not absolutely.

Keywords Conditionally convergent power series • Fekete polynomials

2010 Mathematics subject classification: Primary 30B10; Secondary 30C45, 11C08

1 Introduction

There are power series which on the unit circle converge uniformly but not absolutely.

This was proved in 1913 by Hardy [3], answering a question of M. Riesz. Hardy gave three examples, all closely related to the series $\sum_n n^{-1-i}(\log n)^{-1}z^n$. For the proof he uses a Tauberian argument showing that the partial sums of the series $\sum_n n^{-1-i}z^n$ are uniformly bounded on the unit circle. Hardy remarks that J.E. Littlewood had an elementary proof for the later statement, but this, apparently, was never published. E. Landau in his famous book *Einige neuere Ergebnisse der Funktionentheorie* presents a simplified version of Hardy's proof, cf. Landau-Gaier [5].

Lecture at the meeting *Elementare und Analytische Zahlentheorie,* Blaubeuren, 31.7. – 4.8. 2006

E. Wirsing (✉)
Universität Ulm, Ulm, Germany

Heinrich-Buetzler-Str. 2, 51103 Köln, Germany
e-mail: eduard.wirsing@uni-ulm.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_31

Further proofs have been published since, but all, as far as I know, employ some more or less advanced tools. Thus Gaier [2] elegantly uses the conformal mapping of the unit disk to a region with a rectifiably unreachable boundary point. Herzog and Piranian [4] use lacunary series, Erdős et al. [1] additional combinatorial arguments. A certain similarity to the proof below may be found in the one of Lösch [6] who applies Abel's theorem in its generalization to angular spaces to series of the type $\sum_\nu \frac{(-1)^\nu}{\nu} E^{k_\nu}(z)$ with $E(z) = 1 - \sqrt{1-z}$ and suitably growing k_ν.

At a conference in Colfosco in 2004 W. Luh lectured on a proof of his that is elementary and quite easy. It was this one that inspired me to the one presented in this note. We start from first principles *and* do not require any calculation.

2 The Proof

For polynomials P over $\mathbb{C}$ let

$$\begin{aligned} M(P) &:= \text{the maximum of } |P(z)| \text{ on the unit circle,} \\ A(P) &:= \text{the sum of the absolute values of the coefficients.} \end{aligned}$$

Both of these functionals stay unchanged if $P(z)$ is replaced by $z^n P(z)$ or $P(z^m)$. Moreover $Q(P) := M(P)/A(P)$ for $P \neq 0$ does not change if P is multiplied with a nonzero constant. Obviously $Q(P) \leq 1$.

Lemma 2.1 *For any $\varepsilon > 0$ there are polynomials P such that $Q(P) \leq \varepsilon$.*

To derive Hardy's result from the lemma pick polynomials P_k such that $Q(P_k) \leq 1/k$, normalize them so that $A(P_k) = 1/k$ and, consequently, $M(P_k) \leq 1/k^2$, and line them up nonoverlapping into a power series $\sum_n a_n z^n$ by making

$$\sum_{n_k < n \leq n_{k+1}} a_n z^n \;=\; z^{n_k+1} P_k(z)$$

with suitable n_k. This series does not converge absolutely on $|z| = 1$ since

$$\sum_n |a_n| \;=\; \sum_k A(P_k) \;=\; \sum_k \frac{1}{k} \;=\; \infty\,.$$

On the other hand, the particular partial sums s_{n_k} do converge uniformly because

$$|s_{n_{k+1}} - s_{n_k}| \;=\; \big|P_k(z)\big| \;\leq\; M(P_k) \;\leq\; \frac{1}{k^2}\,,$$

and an arbitrary s_n is linked to the special s_{n_k} with $n_k < n \le n_{k+1}$ by

$$|s_n - s_{n_k}| \;\le\; A(P_k) \;\le\; \frac{1}{k} \;\to\; 0\,.$$

Thus our power series does converge uniformly on $|z| = 1$. □

To prove the lemma it suffices to produce one polynomial P_1 with $Q(P_1) < 1$, since for any two nonzero polynomials R and S and an exponent $g > \deg R$ we have $A\big(R(z)S(z^g)\big) = A(R) \cdot A(S)$, immediately implying sub-multiplicativity $Q\big(R(z)S(z^g)\big) \le Q(R) \cdot Q(S)$. Thus for any $g > \deg P_1$ the recursion

$$P_{k+1}(z) \;:=\; P_1(z)P_k\big(z^g\big) \quad \text{for} \quad k \ge 1$$

generates a sequence of polynomials with $Q(P_k) \le Q(P_1)^k \to 0$.

Actually $Q(P) = Q(c_0 + \cdots + c_d z^d) = 1$ is but an exception if $d \ge 2$. If we allow nonzero c_n only, then at the place a of the maximum ($|a| = 1$) the equation $|\sum_n c_n a^n| = \sum_n |c_n|$ cannot hold unless all $a^n c_n/c_0$ are positive, and in particular, hence, $c_0 c_2/c_1^2 > 0$. □

3 Remark

Polynomials with small quotient Q are known. A nice example are the Fekete polynomials, that are built with the Legendre symbol (here for primes p):

$$F_p(z) \;:=\; \sum_{n=1}^{p-1} \Big(\frac{n}{p}\Big) z^n\,,$$

for which one can show quite elegantly that

$$Q(F_p) \;\ll\; \frac{\log p}{\sqrt{p}}\,.$$

What one needs is essentially that the Gauß sums have modulus $\sqrt{p}$. But that, of course, is an "advanced tool".

References

1. P. Erdős, F. Herzog, G. Piranian, Schlicht Taylor series whose convergence on the unit circle is uniform but not absolute. Pac. J. Math. **1**, 75–82 (1951)
2. D. Gaier, Schlichte Potenzreihen, die auf $|z| = 1$ gleichmäßig, aber nicht absolut konvergieren. Math. Z. **57**, 349–350 (1953)

3. G.H. Hardy, A Theorem concerning Taylor's series. Q. J. Pure Appl. Math. **44**, 147–160 (1913)
4. F. Herzog, G. Piranian, Sets of convergence of Taylor series I. Duke Math. J. **16**, 529–534 (1949)
5. E. Landau, D. Gaier, *Darstellung und Begründung einiger neuerer Ergebnisse der Funktionentheorie* (Springer, Heidelberg, 1986)
6. F. Lösch, Über das Verhalten der Potenzreihen auf dem Rande des Konvergenzkreises III. Math. Z. **37**, 85–89 (1933)

Regular Dessins with Abelian Automorphism Groups

Jürgen Wolfart and Benjamin Mühlbauer

Dedicated to the memory of Wolfgang Schwarz

Abstract A quasiplatonic curve can be defined over the rationals if it has a regular dessin with abelian automorphism group.

Keywords Dessin d'enfant • Quasiplatonic curve

2010 Mathematics subject classification: Primary 11G32; Secondary 14H57

1 Basic Facts and Definitions

The following facts and definitions are fundamental for the theory of dessins d'enfants on Riemann surfaces. Proofs and more details may be found in [11] and the references given there.

1. Compact Riemann surfaces Y are smooth projective algebraic curves, holomorphic mappings between such Riemann surfaces are morphisms between the algebraic curves.
2. As a curve, Y can be defined over a number field if and only if there is a *Belyĭ function* $\beta : Y \to \hat{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$ on Y, that is a meromorphic function, non-constant and ramified at most above $0, 1, \infty$ [1, 7, 9, 12]. In this case we call Y a *Belyĭ surface* or a *Belyĭ curve*, (Y, β) a *Belyĭ pair*.
3. The β-preimage of the real interval $[0, 1]$ defines a bipartite graph on Y with $\beta^{-1}(0)$ and $\beta^{-1}(1)$ as the sets of white and black vertices, respectively. The

Both authors were supported by the DFG project Wo 199/4–1.

J. Wolfart (✉) • B. Mühlbauer
Institut für Mathematik der Goethe Universität, 60629 Frankfurt a.M., Germany
e-mail: wolfart@math.uni-frankfurt.de

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9_32

graph subdivides Y into simply connected cells, and we can consider the poles of β as their midpoints. This embedded graph $\mathscr{D}$ is called the *dessin d'enfant* [8] corresponding to β.

4. On the other hand, if we embed a bipartite graph $\mathscr{D}$ in a compact oriented 2-manifold Y such that $Y \setminus \mathscr{D}$ is the disjoint union of simply connected cells, then there is a unique conformal structure on Y and a unique Belyĭ function β corresponding to $\mathscr{D}$ ([8, 14] or [11, Theorem. 3.15]).
5. For every Belyĭ pair (Y, β), that is for every dessin, there are cocompact Fuchsian triangle groups Δ and finite index subgroups $\Phi \leq \Delta$ such that $Y \cong \Phi\backslash\mathbb{H}$ where $\mathbb{H}$ denotes the hyperbolic plane and such that the Belyĭ function can be written ([17, Theorem. 3], [11, Theorem. 3.10]) as the canonical mapping

$$\Phi\backslash\mathbb{H} \;\to\; \Delta\backslash\mathbb{H} \;\cong\; \hat{\mathbb{C}} \;:\; \Phi z \;\mapsto\; \Delta z \quad .$$

   The entries in the signature (l, m, n) of Δ are common multiples of the zero orders of β, $1-\beta$ and $1/\beta$, respectively. If l, m, n are chosen minimally, we call (l, m, n) the *type* of the dessin. For some triples of small numbers Δ will be an Euclidean or a spherical triangle group and $\mathbb{H}$ has to be replaced with $\mathbb{C}$ or the Riemann sphere $\hat{\mathbb{C}}$.
6. The dessin is called *regular* if there is a group $G \leq \operatorname{Aut} Y$ acting transitively on the set of edges of $\mathscr{D}$ and preserving the colours of the vertices. If Y has a regular dessin, it is called *quasiplatonic* (or *curve with many automorphisms* in older papers, *triangle curve* in the literature about Beauville surfaces). There are many other characteristic properties ([17] or [11, Theorem. 5.1]), for example

   – the Belyĭ function β defines a normal covering,
   – its monodromy group (the so-called *cartographic group* of the dessin) is isomorphic to its covering group,
   – Φ is a normal subgroup of Δ, and one has $\Delta/\Phi \cong G$.

   Every Belyĭ surface (or every dessin) has a quasiplatonic (respectively regular) covering of finite degree.
7. The field L is called a *field of definition* for Y if all coefficients of the polynomials defining Y are contained in L. More generally, we call L a field of definition for Y if there is a curve Y' isomorphic (over $\mathbb{C}$) to Y defined over L. For $\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$ we denote by Y^σ the curve obtained by the action of σ on all coefficients of the defining equations of Y. In the context of the present paper, we may suppose that L is a number field; it is not at all uniquely determined, however the *moduli field* $M(Y)$ of Y, that is the fixed field of the subgroup

$$V_Y \;:=\; \{\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q} \mid Y^\sigma \cong Y\} \;\leq\; \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$$

   of the absolute Galois group depends only on the isomorphism class of Y. It is contained in all fields of definition of Y. For any number field K we can define similarly a field of definition $\geq K$ and a moduli field $M_K(Y, G)$ for the pair

consisting of Y and a group $G \leq \operatorname{Aut} Y$ of automorphisms as the fixed field of the group

$$V_{(Y,G)/K} := \{\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/K \mid \exists f_\sigma : Y \to Y^\sigma \text{ isomorphism with } f_\sigma \circ \alpha = \alpha^\sigma \circ f_\sigma \forall \alpha \in G\}. \tag{1.1}$$

8. It is well known that the moduli field is not always a field of definition of Y [5, 13]. According to Weil [16] it is a field of definition if there is a choice of isomorphisms $f_\sigma : Y \to Y^\sigma$ for all $\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/M(Y)$ satisfying the *cocycle condition*

$$f_{\sigma\tau} = f_\sigma^\tau \circ f_\tau \quad \text{for all} \quad \sigma, \tau \in \operatorname{Gal}\overline{\mathbb{Q}}/M(Y) \quad .$$

9. By consequence, Y can be defined over $M(Y)$ if the identity is the only automorphism of Y because then all f_σ are uniquely determined. By variations of this argument, also regular dessins, that is Belyĭ pairs (Y, β) with normal β can be defined over their moduli field $M(Y, \beta)$ [3, Proposition 2.5], obviously defined as the fixed field of

$$V_{(Y,\beta)} := \{\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q} \mid \exists f_\sigma : Y \to Y^\sigma \text{ isomorphism with } \beta^\sigma \circ f_\sigma = \beta\} .$$

From this result one can derive that also quasiplatonic curves can be defined over their moduli field ([4], [17, Theorem 5], [11, Theorem 5.4]). Similarly, $(Y, \operatorname{Aut} Y)$ can be defined over its moduli field if $\operatorname{Aut} Y$ contains its centre as a direct factor [6, Theorem 1].

2 Abelian Automorphism Groups

Theorem 2.1 *Let $\mathscr{D}$ be a regular dessin on a quasiplatonic curve X with abelian automorphism group $\operatorname{Aut}\mathscr{D}$, and let β denote the corresponding Belyĭ function. Then, (X, β) is defined over $\mathbb{Q}$.*

Corollary *Quasiplatonic curves having a regular dessin with abelian automorphism group can be defined over $\mathbb{Q}$.*

Theorem 2.1 is already given as Proposition 3 in [2], together with a sketch of a proof. For the corollary, and under slightly different hypotheses, there are two more recent proofs in [10] and [15, Corollary 1.2], based on quite different ideas. We will use instead the following lemma which seems to be well known; unfortunately, we do not know a quotable source or where it originally comes from (the first author learned it from David Singerman and Gareth Jones many years ago).

Lemma *Every regular dessin $\mathscr{D}$ with abelian automorphism group is a quotient of some regular dessin $\mathscr{D}_r$ of type (r,r,r) on the Fermat curve F_r of exponent r, with automorphism group* $\operatorname{Aut}\mathscr{D}_r \cong C_r \times C_r$.

Proof (See also [11], Example 5.5 and Exercise 5.8) If we describe F_r by its affine model $x^r + y^r = 1$, it is easy to see that $\beta(x,y) := x^r$ defines a normal Belyĭ function corresponding to the normal inclusion $\Delta' \lhd \Delta$ of the commutator subgroup in the triangle group $\Delta = \Delta(r,r,r)$. This commutator subgroup is the surface group of F_r, and for the corresponding dessin $\mathscr{D}_r$ we have

$$\operatorname{Aut}\mathscr{D}_r \;\cong\; \Delta/\Delta' \;\cong\; C_r \times C_r$$

(for $r > 3$ it is an index 6 normal subgroup of the full automorphism group $\operatorname{Aut}F_r$). Now suppose that X is quasiplatonic with a regular dessin of type (l,m,n) and abelian automorphism group A. Let r be the lcm of l,m,n. The surface group N of X is then the (torsion free) kernel of a group epimorphism of the triangle group $\Delta(l,m,n)$ onto A, inducing as well an epimorphism

$$\Delta = \Delta(r,r,r) \;\to\; A$$

with some kernel $\Gamma \lhd \Delta$ which is in general not torsion free. We have however $X \cong \Gamma\backslash\mathbb{H}$, and because $A \cong \Delta/\Gamma$ is abelian, we get $\Delta' \lhd \Gamma$ with a quotient $\Gamma/\Delta' =: U \lhd C_r \times C_r$, whence

$$X \cong U\backslash F_r \quad \text{and} \quad \mathscr{D} \cong U\backslash\mathscr{D}_r\,.$$

□

Proof of Theorem 2.1 With the same notations and the same affine model for F_r as above we have now $X \cong U\backslash F_r$. Every automorphism $\alpha \in U$ acts on F_r by

$$\alpha \;:\; (x,y) \;\mapsto\; (\zeta_r^k x, \zeta_r^h y)$$

with a primitive r-th root of unity ζ_r and exponents $k,h \in \mathbb{Z}/r\mathbb{Z}$. So, F_r and its Belyĭ function β are defined over $\mathbb{Q}$ and $\operatorname{Aut}F_r$ is defined over $\mathbb{Q}(\zeta_r)$. Moreover, the Belyĭ function B on X can be considered as induced by the Belyĭ function β on the U-orbits in F_r (well defined because β has the same value for all arguments in every U-orbit). Clearly, $X^\sigma = U^\sigma\backslash F_r$ for all $\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$ where σ acts in the obvious way on the automorphisms $\alpha \in U$, hence B^σ is induced by β on the U^σ-orbits. However, since every Galois automorphism $\sigma \in \operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$ acts on ζ_r as $\zeta_r \mapsto \zeta_r^s$ for some $s \in \mathbb{Z}/r\mathbb{Z}$ only depending on σ, we have $\alpha^\sigma = \alpha^s$ and $\alpha^\sigma \in U$ for all $\alpha \in U$, hence $U^\sigma = U$ for all σ. Because $\mathscr{D}_r$, that is the pair (F_r,β) is defined over $\mathbb{Q}$, also the quotient $\mathscr{D} = U\backslash\mathscr{D}_r$ is invariant under $\operatorname{Gal}\overline{\mathbb{Q}}/\mathbb{Q}$. Therefore its moduli field is $\mathbb{Q}$, and by Proposition 2.5 of [3] (see point (9) of Sect. 1) $\mathscr{D}$ can be defined over $\mathbb{Q}$. □

3 Examples and Generalisations

Quasiplatonic surfaces having dessins with abelian automorphism groups exist in all genera $g > 1$, compare the Accola–Maclachlan curves described in [11, Exercise 5.20]: for $n = 2g + 1$ the automorphism group $A \cong C_{2n}$ is an image of the triangle group $\Delta(2, n, 2n)$ under an epimorphism with torsion free kernel Γ such that the quotient curve $X \cong \Gamma\backslash\mathbb{H}$ has an affine model

$$y^2 = x^n - 1 \quad .$$

In fact, there are much more examples. Among the 22 isomorphism classes of quasiplatonic curves in the genera $g = 2, 3, 4$ there are only one curve in genus 3 and three curves in genus 4 not having a regular dessin with abelian automorphism group (they are also defined over $\mathbb{Q}$, but by other reasons, compare [2]), see the Tables 5.2–5.4 in [11].

Recall that a curve Y of genus > 1 has only finitely many automorphisms. If Y is defined over a number field K, its automorphisms can therefore also be defined over a fixed number field $L \geq K$: by the action of field automorphisms of $\mathbb{C}$ on $\mathrm{Aut}\, Y$ fixing K elementwise we would otherwise get an infinity of automorphisms. A similar argument shows that a minimally chosen L is a normal extension of K. Recall also that $Y = \Gamma\backslash\mathbb{H}$ for a torsion-free normal subgroup $\Gamma \lhd \Delta$ of the triangle group Δ which is the normaliser of Γ in $\mathrm{PSL}_2\,\mathbb{R}$.

Theorem 3.1 *Let Y be a quasiplatonic curve, β its canonical Belyĭ function $Y \to \mathrm{Aut}\, Y\backslash Y$, let K be the moduli field (= minimal field of definition) of (Y, β), and let the Galois extension $L \geq K$ be a field of definition for $(Y, \mathrm{Aut}\, Y)$.*

(1) For any subgroup $U \leq \mathrm{Aut}\, Y$, the curve $X := U\backslash Y$ and the Belyĭ function B induced by β on X can be defined over L.

(2) Its relative moduli field $M_K := M_K(X, B)$, defined as the fixed field of

$$V_{(X,B)/K} := \{\sigma \in \mathrm{Gal}\,\overline{\mathbb{Q}}/K \mid \exists f_\sigma : X \to X^\sigma \text{ isomorphism with } \quad B^\sigma \circ f_\sigma = B\},$$

is the same as the fixed field of the group

$$G_U := \{\sigma \in \mathrm{Gal}\, L/K \mid U^\sigma \text{ is conjugate to } U \text{ in } \quad \mathrm{Aut}\, Y\} \quad .$$

Proof 1. Can be proved similarly to Corollary 1 of [6] considering the intermediate fields in the function field extension $L(Y)/L(\beta)$ whose Galois group[1] is antiisomorphic to $\mathrm{Aut}\, Y$, compare [11, Theorem 4.5].

[1] Girondo et al. [6] contains a little mistake: since β is used in the base field of the Galois extension of function fields, we have to be sure that β is also defined over the field of constants; this is guaranteed here by the construction of $K \leq L$. In Corollary 1 of [6] this may fail if the hypotheses of Lemma 1 or Lemma 2 of [6] are not satisfied. There one can fill the gap in the hypothesis by

2. First we have to prove that if there is an $a \in \operatorname{Aut} Y$ with the property $aUa^{-1} = U^\sigma$, we get an isomorphism

$$f : U\backslash Y = X \to X^\sigma = U^\sigma\backslash Y \quad \text{with } B = B^\sigma \circ f$$

which is in fact induced by $Y \to Y : y \mapsto a(y)$. Second we have to show that for any $\sigma \in \operatorname{Gal} L/K$ with the property $(X^\sigma, B^\sigma) \cong (X, B)$ there is such an automorphism $a \in \operatorname{Aut} Y$ inducing this isomorphism via the conjugation of U, hence $\sigma \in G_U$. Since σ fixes Y and β, both subgroups U and U^σ lift to Fuchsian groups Φ, Φ^σ between Γ and Δ. The isomorphism $f : X \to X^\sigma$ lifts to some $\alpha \in \mathrm{PSL}_2\,\mathbb{R}$ acting on $\mathbb{H}$ and conjugating Φ into Φ^σ since $B = B^\sigma \circ f$. Moreover, α normalises Γ, hence belongs to Δ and induces an automorphism $a \in \operatorname{Aut} Y$.

□

If $U \lhd \operatorname{Aut} Y$ is a normal subgroup, X is itself quasiplatonic. If moreover $K = \mathbb{Q}$, then M is the minimal field of definition of (X, B).

References

1. G.V. Belyĭ, On Galois extensions of a maximal cyclotomic field. Izv. Akad. Nauk SSSR Ser. Mat. **43**, 267–276, 479 (1979)
2. M.D.E. Conder, G.A. Jones, M. Streit, J. Wolfart, Galois actions on regular dessins of small genera. Rev. Mat. Iberoam. **29**, 163–181 (2013)
3. K. Coombes, D. Harbater, Hurwitz families and arithmetic Galois groups. Duke Math. J. **52**, 821–839 (1985)
4. P. Dèbes, M. Emsalem, On fields of moduli of curves. J. Algebra **211**, 42–56 (1999)
5. C.J. Earle, On the moduli of closed Riemann surfaces with symmetries, in *Advances in the Theory of Riemann Surfaces*, ed. by L.V. Ahlfors et al. Annals of Mathematics Studies, vol. 66 (Princeton University Press, Princeton, 1971), pp. 119–130
6. E. Girondo, D. Torres-Teigell, J. Wolfart, Fields of definition of uniform dessins on quasiplatonic surfaces, in *Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces*, ed. by M. Izquierdo et al. Contemporary Mathematics, vol. 629 (AMS, Providence, 2014), pp.155–170
7. G. González-Diez, Variations on Belyi's theorem. Q. J. Math. **57**, 339–354 (2006)
8. A. Grothendieck, Esquisse d'un Programme, in *Geometric Galois Actions. 1. Around Grothendieck's Esquisse d'un Programme*, ed. by L. Schneps, P. Lochak. London Mathematical Society Lecture Note Series, vol. 242 (Cambridge University Press, Cambridge, 1997), pp. 5–48
9. H. Hammer, F. Herrlich, A remark on the Moduli field of a curve. Arch. Math. **81**, 5–10 (2003)
10. R. Hidalgo, Homology closed Riemann surfaces. Q. J. Math. **63**, 931–952 (2012)
11. G.A. Jones, J. Wolfart, Dessins d'Enfants on Riemann Surfaces. Springer Mathematical Monographs, Cham (2016)
12. B. Koeck, Belyi's theorem revisited. Beitr. Algebra Geom. **45**, 253–275 (2004)

replacing the moduli field $M(S, G)$ with a—sometimes slightly larger—moduli field $M(S, \beta, G)$ in whose definition all f_σ satisfy in addition $\beta^\sigma \circ f_\sigma = \beta$.

13. G. Shimura, On the field of rationality of an Abelian variety. Nagoya Math. J. **45**, 167–178 (1972)
14. D. Singerman, Automorphisms of maps, permutation groups and Riemann surfaces. Bull. Lond. Math. Soc. **8**, 65–68 (1976)
15. D. Torres-Teigell, Triangle Groups, Dessins d'Enfants and Beauville Surfaces. Ph.D. thesis, Madrid, 2012
16. A. Weil, The field of definition of a variety. Am. J. Math. **78**, 509–524 (1956)
17. J. Wolfart, ABC for polynomials, dessins d'enfants, and uniformization – a survey, in *Elementare und Analytische Zahlentheorie (Tagungsband), Proceedings ELAZ-Conference, May 24–28, 2004*, ed. by W. Schwarz, J. Steuding (Steiner, Stuttgart, 2006), pp. 313–345

Impressions from the $\mathcal{EL}\mathcal{AZ}$ Conference 2014 in Hildesheim

Longtime member of the Frankfurt
Longtime member the Wissenschaftliche Gesellschaft at Frankfurt
Longtime trustee of the Catholic Church's Cusanuswerk at Frankfurt
1972–94 Co-organizer (with H.-E. Richert and E. Wirsing) of the MFI
conferences on Elementary and Analytical Number Theory

Lutz Lucht giving his talk at the memorial colloquium for his friend Wolfgang Schwarz. Published with kind permission of © Jürgen Sander, 2014

© Springer International Publishing Switzerland 2016

J. Sander et al. (eds.), *From Arithmetic to Zeta-Functions*,
DOI 10.1007/978-3-319-28203-9

The program of the Wednesday colloquium in memory of Wolfgang Schwarz during the $\mathcal{ELAZ}$ Conference 2014 in Hildesheim:

Stiftung Universität Hildesheim 2003

Domäne Marienburg

ELAZ 2014

Elementare und Analytische Zahlentheorie

Colloquium in memory of Wolfgang Schwarz

1934 — 2013

Aula (Hohes Haus)

9.00 Jürgen Sander: Address of Welcome

9.05 Lutz Lucht: Remembering Wolfgang Schwarz - his life and work

9.50 Karl-Heinz Indlekofer: Arithmetische Funktionen: ein Schwerpunktthema im wissenschaftlichen Werk von Wolfgang Schwarz

Steinscheune

10.40 Coffee break

Ackerpferdestall

11.10 Eva Schwarz (Violine), Valentin Blomer (Klavier)

W. Schwarz, Romanze für Violine und Klavier

L. v. Beethoven, Sonate G-Dur op. 31/1
Allegro vivace
Adagio grazioso
Rondo - Allegretto

A. Dvorak, Romantische Stücke op. 75, Nr. 1 und 3
Allegro moderato
Allegro appassionato

Aula (Hohes Haus)

11.45 Jörn Steuding: On Liouville Numbers – Yet Another Application of Functional Analysis in Number Theory

Steinscheune

12.30 Lunch

Besides some biographical and scientific lectures the audience was listening to a concert of classical music; see the audience eagerly waiting for the beginning.

Published with kind permission of © Isa Lange, 2014

Published with kind permission of © Isa Lange, 2014

Wolfgang Schwarz's daughter Eva (violin) and Valentin Blomer (piano) were playing some pieces composed by Beethoven, Dvořák, and Schwarz himself.

Published with kind permission of © Isa Lange, 2014

The conference photography below was taken during this special event at the *Domäne Marienburg* of the University of Hildesheim.

Published with kind permission of © Isa Lange, 2014

Published with kind permission of © Jürgen Sander, 2014